

Protective Security at Sea: A Counter Terrorism Framework for Cruise and Passenger Ships

Kuhn, K., McIlhatton, D., Malcolm, J. & Chapsos, I.

Author post-print (accepted) deposited by Coventry University's Repository

Original citation & hyperlink:

DOI 10.1007/s13437-022-00296-w

ISSN 1651-436X

ESSN 1654-1642

Publisher: Springer

The final publication is available at Springer via <http://dx.doi.org/10.1007/s13437-022-00296-w>

Copyright © and Moral Rights are retained by the author(s) and/ or other copyright owners. A copy can be downloaded for personal non-commercial research or study, without prior permission or charge. This item cannot be reproduced or quoted extensively from without first obtaining permission in writing from the copyright holder(s). The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the copyright holders.

This document is the author's post-print version, incorporating any revisions agreed during the peer-review process. Some differences between the published version and this version may remain and you are advised to consult the published version if you wish to cite from it.

Protective Security at Sea: A Counter Terrorism Framework for Cruise and Passenger Ships

Kristen Kuhn^{a,*}, David McIlhatton^a, James A. Malcolm^a and Ioannis Chapsos^a

^a*Centre for Trust, Peace and Social Relations (CTPSR), Coventry University, CV1 2TL, United Kingdom*

ARTICLE INFO

Keywords:

Protective security
Counter terrorism
Maritime
Decision-making
Security governance

ABSTRACT

In the present context of global terrorism, managing protective security in cruise and passenger ships is a challenge for organisations. This is due, in part, to the distinct lack of a counter terrorism framework for the industry. To address this gap, this paper develops a counter terrorism framework for cruise and passenger ships. This framework identifies protective security components and terrorist threats based on known attacks. It provides stakeholders with a means to assess risk, both in terms of likelihood and wider organisational impact. From an operational security perspective, the contribution of the framework is three-fold: First, it offers a consistent approach to delivering an effective protective security posture at all stages of a ship's itinerary. Second, it is envisaged that the application of the framework will improve security decision-making within organisations. Third, improved organisational security may, over time, enhance deterrence.


Statements and Declarations

There are no competing interests that are directly or indirectly related to the work submitted for publication.

Acknowledgements

This research was supported by the NATO Maritime Interdiction Operational Training Centre (NMIOTC).

*Principal corresponding author

 kristen.kuhn@coventry.ac.uk (K. Kuhn); david.mcilhatton@coventry.ac.uk (D. McIlhatton); james.malcolm@coventry.ac.uk (J.A. Malcolm); ioannis.chapsos@coventry.ac.uk (I. Chapsos)

ORCID(s): 0000-0001-8906-0197 (K. Kuhn); 0000-0001-5795-0099 (D. McIlhatton); 0000-0003-0446-7620 (J.A. Malcolm); 0000-0003-3784-1578 (I. Chapsos)

Noname manuscript No.
(will be inserted by the editor)

Protective Security at Sea: A Counter Terrorism Framework for Cruise and Passenger Ships

the date of receipt and acceptance should be inserted later

Abstract In the present context of global terrorism, managing protective security in cruise and passenger ships is a challenge for organisations. This is due, in part, to the distinct lack of a counter terrorism framework for the industry. To address this gap, this paper develops a counter terrorism framework for cruise and passenger ships. This framework identifies protective security components and terrorist threats based on known attacks. It provides stakeholders with a means to assess risk, both in terms of likelihood and wider organisational impact. From an operational security perspective, the contribution of the framework is three-fold: First, it offers a consistent approach to delivering an effective protective security posture at all stages of a ship's itinerary. Second, it is envisaged that the application of the framework will improve security decision-making within organisations. Third, improved organisational security may, over time, enhance deterrence.

Keywords Protective security · Counter terrorism · Maritime · Decision-making · Security governance

1 Introduction

It has been nearly four decades since Leon Klinghoffer, a 69-year-old Jewish-American man, was shot and thrown overboard the *MS Achille Lauro*, an Italian-flag cruise ship [20]. The ship was hijacked in 1985, en-route from Egypt to Israel, by four heavily armed members of the Palestinian Liberation Front (PLF) in what turned into a two-day ordeal. This is a high-profile case of terrorism on cruise ships, a topic which is often overshadowed by traditional maritime security threats, such as piracy. However, while threats like piracy are well understood and have changed little in practice [30], the threat of terrorism is complex and evolving. This

presents challenges to maritime organisations which aim to protect cruise and passenger ships against terrorist threats. These challenges are exacerbated by the distinct lack of a counter terrorism framework for these ships, with which industry stakeholders can identify and counter terrorist threats.

One such challenge includes that none of the international legal instruments that are directly or indirectly relevant to maritime terrorism define the term ‘maritime terrorism’ [28]. While researchers have attempted definitions, including “*the systematic use or threat to use acts of violence against international shipping and maritime services by an individual or group to induce fear and intimidation in a civilian population in order to achieve political ambitions or objectives*” [27], there is no generally accepted legal definition of maritime terrorism. In contrast, while there is no such agreed upon definition of piracy under international law [19] the definition of piracy in Article 101 of UNCLOS, [54]– which established the key facets of piracy as that it is (i) committed for private ends, (ii) takes place on the high seas and (iii) done by one ship on another ship [2]– is widely accepted [58]. For this reason, acts of maritime terrorism may be treated as piracy even though key distinctions exist between them in relation to differing motivations and objectives [52], as was the case in the 1985 *MS Achille Lauro* incident [20]. However, protective security is not concerned with differing motivations but rather shared capabilities. Consider that in the moment of an attack it is often the case that the threat actor (and their motivation) is unclear. A counter terrorism framework would benefit not only efforts to counter maritime terrorism but also efforts to counter other violent acts (such as piracy) in the maritime domain.

The rationale behind this research is to create the first end-to-end counter terrorism framework for assessing terrorist risk in cruise and passenger ships. The need to protect cruise and passenger vessels is recognised by the international community, as evidenced by the International Ship and Port Facility (ISPS) Code [25] which introduces provisions (both mandatory and recommendatory) to protect people and places. The ISPS Code was developed through the auspices of the International Maritime Organization (IMO) and was adopted on 12th December 2002, with compliance with the code being mandatory from 1st July 2004 for all contracting states to the International Convention for the Safety of Life at Sea (SOLAS) [25]. The ISPS Code represented a significant development in the regime through which risk and security was handled in the maritime industry in the context of international terrorism [38]. However, the code is limited in its consideration of the protection of information, and it is limited in that it only applies to some merchant vessels engaged on international voyages (i.e., not domestic passenger ferry services) and those port facilities that serve them, unless contracting governments extend its application. Other developments related to the protection of information include two IMO legal instruments adopted in 2017: a non-mandatory cyber-guideline [23] and a resolution on the application of the international safety management code (ISM) Code [24]. However, many agree “*maritime cybersecurity is yet to get*

1 *proper attention on the IMO agenda*” and so legal instruments on maritime
2 safety, security and facilitation of maritime traffic have become relevant in a
3 legal context for maritime cybersecurity [29]. The ambiguous use of such
4 guidelines, as demonstrated in the case of cybersecurity, underscores the
5 need for a comprehensive protectively security framework which not only
6 acknowledges but synthesises existing efforts to look at information security
7 on ships- and further pulls together on land and at sea activities.

8
9 The originality of this paper stems from the lack of research and
10 regulation addressing terrorism holistically at the land-sea nexus, both in
11 terms of components to protect and in its application. Moreover, the
12 proposed framework considers security challenges specific to cruise and
13 passenger ships, where the characteristics of the industry itself shape the risk
14 profile. For instance, unlike traditional crowded places which are often fixed
15 in one location, the type of threats faced by the cruise ship industry are
16 dynamic and highly complex due to the multiple locations they visit, the
17 long periods of time they spend at sea, and the high volume of passengers
18 that they accommodate. Consequently, this paper aims to satisfy a gap in the
19 current body of maritime security research, where we have identified a need
20 to relate existing protective security postures for land-based crowded places
21 to cruise and passenger ships. Our understanding of crowded places becomes
22 multi-dimensional in the cruise and passenger ship context, a situation that
23 we acknowledge in the conceptualisation of our counter terrorism framework.

24
25 The contribution of this research is three-fold: First, it offers a consistent
26 approach to delivering an effective protective security posture at all stages of
27 a ship’s itinerary. This allows industry stakeholders to identify and counter
28 terrorist threats. Second, in doing so, it is envisaged that the application of
29 the framework will improve security decision-making within organisations.
30 Third, improved organisational security has the potential, over time, to
31 enhance deterrence. The rest of this paper is organised as follows: Section 2
32 identifies the protective security components for cruise and passenger ships,
33 which include people, places and information. Section 3 outlines terrorist
34 threats associated with cruise and passenger ships, drawing on six known
35 attacks. Section 4 bring together these components and threats to examine
36 how terrorist risks are assessed in terms of likelihood and impact. Section 5
37 examines response in the context of effective decision-making. Section 6
38 considers the importance of evaluation. Section 7 presents the first counter
39 terrorism framework for cruise and passenger ships. Section 8 outlines
40 conclusions and suggests future work.

41 42 43 44 **2 Protective Security Components for Cruise and Passenger Ships**

45
46 The UK Centre for the Protection of National Infrastructure (CPNI) [8]
47 indicates that the most effective way for an organisation to protect itself
48 against security threats is to use a combination of physical, personnel and
49 people, and cyber security measures. It is key to note that these components
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

are interconnected and should be approached holistically to ensure effective risk assessment. This is because the risk of various threats exist simultaneously and there also exists the possibility of hybrid attacks. To adopt an integrated security approach, these groups inform the three components of protective security for cruise and passenger ships proposed in the paper, which include: people, places and information.

2.1 People

Cruise and passenger ships are lucrative targets for terrorists due to the density of passengers on-board [45], not unlike commercial aviation. However, while counter terrorism and aviation security received significant attention following the attacks of September 11, 2001, which resulted in the deaths of nearly 3000 people [51], maritime security received less attention. A notable exception was the ISPS Code [25] which, amongst other things, requires the introduction of Ship Security Officers on passenger ships engaged on international voyages. For this reason, this paper develops an understanding of people security based on those established outside the cruise ship industry, and then applies it. While CPNI [8] refers to “personnel and people security” this paper refers simply to “people” under the pretext that personnel are also people. People security focuses on two integrated work-streams that aim, first, to reduce the risk of employees exploiting their position, trust, and access, either intentionally or unintentionally, for reasons that adversely impact on their organisation, its competitiveness, society or national security. Second, people security is concerned with developing and enabling an effective security culture that minimises the potential for vulnerabilities to be exposed and exploited.

2.2 Places

Whereas the previous component is concerned with people, this component focuses on places which includes the physical protection of buildings and spaces. Protective security takes place at sea as it does on land, yet little attention in research has been placed on making connections between the domains. Addressing this gap is particularly important for the cruise and passenger ship industries because they are places that both create and connect urban and maritime crowded places.

Passengers and crew (the crowd) regularly navigate the land-sea nexus during a cruise, with respect to the “the three sides of the coin:” ship, shore and their connections [26]. Cruise ships are often stationary for relatively long periods of time [55], either anchored offshore to enable passengers to go on excursions on-shore, or docked in port before the journey starts, at each main stop, and at the end of their itinerary. As a result, the protective security umbrella needs to be spatially comprehensive with a greater

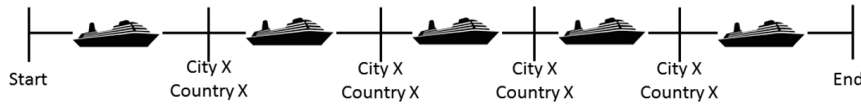


Fig. 1: Multi-node dynamic system, which depicts the itinerary of a cruise or passenger ship across time and space, whereby a ship may make any number of stops or excursions. In order to understand the risks faced by these ships, the ship's itinerary can be categorised in to five stages: (1) In Port – before journey commences, (2) At Sea - between stops, (3) At Stop (n) – in port, (4) At Stop (n) – visitor excursions, (5) In Port – end of journey

consistency of approach across multiple locations. In terms of existing regulation, the ISPS Code [20] recognises the need to secure multiple spaces, requiring the introduction of restricted areas where people and goods move on and off vessels (the ship-port interface), alongside security plans for applicable vessels and the facilities that serve them. Overall, to understand the risks faced by cruise and passenger ships, one must therefore assess risk at all stages in a ship's itinerary shown in Figure 1.

We also recognise that counter-terrorism activity outside this multi-node system influences both the terrorist threat profile and protective security response in relation to cruise and passenger ships. For example, a study in the United Kingdom argued that *“the counter-terrorism security response in relation to ports could be described as constantly evolving, layered and increasingly expansive in scope”* [34] with policymakers and security practitioners interested in pushing threats further away from infrastructure deemed to be particularly important and vulnerable to attack. However, it is necessary to establish some boundaries to the scope of any framework in order facilitate depth of analysis and maintain coherence. As a result, we regard activities outside the multi-node system beyond the direct scope of the proposed framework, even though we accept that when the framework is operationalised, the wider security context in any given case will need to be considered.

To further explore the terrorism risk profile associated with cruise and passenger ships, it is useful to explain how we understand crowded places, the way these ships encapsulate them and why they are significant locations for terrorist action. The extant literature presents little in the way of an agreed definition for ‘crowded places’ with most research adapting those that emerge from government taxonomies. In line with the crowded places guidance put forward by the UK Government [39], McIlhatton et al. [36] consider crowded places to include entertainment complexes, stadia, bars, pubs, nightclubs, hotels, shopping malls, places of worship, iconic sites, urban spaces and educational institutes. Other definitions are broader, with the Australian Government [14] articulating in their definition that crowded

places “*do not have to be buildings*” and thus may include ships. It is also interesting to note that, in line with this definition, cruise ships take on large numbers of people “*on a predictable basis*.” In the context of terrorism, this is key for planning attacks, thus increases its attractiveness as a target.

While none of the definitions offered on crowded places explicitly refer to cruise and passenger ships, and instead refer to sub-sectors of transport within their crowded places nomenclatures, this paper suggests that such vessels should be considered as a core inclusion in crowded places strategies related to counter terrorism. This stems from the notion that cruise ships often have large crowds of people (cruise ships can now hold over 5,000 passengers), include many of the same elements as ‘traditional’ crowded places (pubs, restaurants, entertainment complexes, shopping malls, theatres, etc.), and generate large crowds of people at each port of call. Indeed, in the United Kingdom, a focus on improving the awareness of the potential terrorism threat posed in crowded places through scenario activities (Project Argus) has been utilised in a port setting [33].

Although it becomes clear that passenger and cruise ships fit within the provided definitions of crowded places, what makes them distinct from land-based venues is that they are not static within a state’s territory. Ships usually transit through different maritime zones (such as territorial waters and international waters) and call at different (potentially international) ports, as seen in Figure 1. This adds a layer of complexity in the legal jurisdictions involved, as different requirements and regulations exist within each coastal state’s territorial waters, in the open seas and each individual port state. As a result, different legal obligations may exist and various stakeholders may be responsible for response and decision-making throughout a ship’s itinerary. However, the principal legal and testing responsibilities of the proposed framework mainly lie with the vessel including the ship’s flag state. While the different legal jurisdictions within the ships’ multi-node dynamic system are acknowledged, it goes beyond the conceptual nature and scope of this paper to analyse them in depth. As such, it considers the implementation and testing of this framework to remain, in the first instance, each flag state’s responsibility, irrespective of the coastal state and port state regulations within the ship’s itinerary.

2.3 Information

Digital acceleration, advancements in technology and wider access to data have substantially enhanced the level of information available on cruise and passenger ships. While these technologies provide opportunities for organisations to boost business and customer satisfaction through increasingly advanced customer experiences, they also increase risk [32]. For instance, most cruise ship itineraries are available online providing a comprehensive understanding of where ships will be, and when, making them more predictable. The growth of location-based information in an

open-source manner has resulted in the ability to track cruise ships in real-time which poses challenges for those managing terrorism risk. Further, emerging technologies such as virtual/augmented/mixed realities enable prospective customers to virtually tour ships in advance of their selection, using high resolution 360-degree imagery which is openly available online. These developments have created new security challenges for those managing risk within cruise and passenger ships. Such developments as a virtual tour can be taken not only by prospective passengers, but also threat actors. Thus, hostile reconnaissance has shifted from an analogous to a digital environment where the attacker does not have to be present. This poses questions for future training and poses challenges to identifying hostile reconnaissance and attribution.

At large, existing regulation in the cruise and passenger ship industry does not holistically address the need to protect information due to a lack of clear and enforceable security applications. First, in terms of clarity, information security is important and requires users to be aware of existing legislation in their space, yet this is not always the case. For example, the European Union's General Data Protection Regulation (GDPR) [41] is widely known since it came into effect on 25 May 2018, but the rules in the GDPR on its territorial (and extra-territorial) scope are not. Other research [31] examines the application of the GDPR in complex scenarios, with particular attention to non-EU companies, groups of companies and those which offer software-as-a-service. Here, Korff (2019) highlights cruise ships as *"a special case"* as:

"the offering of and providing of cruises will involve more than "the ship": the cruise is likely to be offered to the prospective customers by a company specialising in such travel– and that company is likely to be part of a wider group of companies, some of which may be based in the EU/EEA, and some not."

GDPR regulations may apply to the shore-based operations of cruise ship companies and to ships at sea (which they may or may not own). However, due to the complexity of such scenarios, the clarification of the different roles and responsibilities of each entity– and if, how and to what extent the GDPR applies to them– should be considered on a case-by-case basis.

Second, to ensure accountability to such legislation, it is important that such regulatory tools are enforced. For instance, the ISPS Code [25] has no mandatory cybersecurity provisions, explicit or implicit, but encourages port facilities to consider *"radio and telecommunications equipment, including computer systems and networks"* when they assess physical security vulnerabilities. Hinting at the need for some stakeholders to consider protecting information is a notable aspiration, but it does not offer an enforceable security application.

3 Attacks on Cruise and Passenger Ships

Table 1: Types of terrorist threat vectors and illustrative examples of known attacks on cruise and passenger ships

Threat vector	Illustrative Example of Known Attack
Biological Attack*	<i>MS Carnival Magic</i> [16]
Cyber Attack*	Carnival Cruises [35]
Fire as a Weapon (FAW)	<i>MS Our Lady of Mediatrix</i> [46]
Hijacking	<i>MS Achille Lauro</i> [20]
Improvised Explosive Devices (IED) Attack	<i>MV SuperFerry 14</i> [50]
	<i>MS Our Lady of Mediatrix</i> [46]
	<i>MS City of Poros</i> [18]
Insider Threat	<i>MS Carnival Magic</i> [16]
Marauding Terrorist Attack (MTA)	<i>MS City of Poros</i> [18]

*These threat vectors have been used by other threat actors on cruise and passenger ships, but not by terrorists to date

Having examined the range of components involved in protective security for cruise and passenger ships, attention can turn to the terrorist threats faced by such vessels. While acknowledging these threats are complex and dynamic, this paper draws on known attacks to create a list of probable and potential terrorist threats to cruise and passenger ships, as seen in Table 1. These attacks are not exhaustive but have been selected thoughtfully to illustrate the full range of threats terrorists could pose to cruise and passenger ships.

As terrorist threats are complex, some known attacks make use of multiple threat vectors to include a hybrid attack. For instance, in the case of *MS City of Poros* [18], a failed improvised explosive devices (IED) attack was followed by a successful marauding terrorist attack (MRA). Terrorists may exploit multiple vulnerabilities and use more than one threat vector in a single attack, in order to increase their chance of success. This example also highlights the fact that not all attempts by terrorist are successful. This paper examines attacks that are both successful and otherwise, as both demonstrate intent to harm.

As terrorist threats are dynamic, threat vectors may evolve over time. To envision new potential terrorist threats facing cruise and passenger ships, this paper departs from the probable (known terrorist attacks on cruise and passenger ships) to consider the potential threats by different threat actors in the same domain. For instance, we consider cyber attacks on cruise and passenger ships, even though they were not perpetrated by terrorists. This is because even though there are no known cyber attacks by terrorists to date, the threat vector has been successfully demonstrated on the target and could be adopted by terrorists.

3.1 Carnival Cruises

According to the Danish Defence Intelligence Service (DDIS) [17], cyber terrorism is defined as cyber attacks aimed at creating effects similar to those of conventional terrorism, including cyber attacks causing personal injury or major disruptions in critical infrastructure. Ransomware and other forms of cyber attacks have reportedly been on the rise in 2020 [35] with the maritime industry being one of the latest targets for hackers. Carnival Corporation, a cruise operator, was hit by a ransomware virus twice in two years (2019-2020) [35]. Both attacks are likely to have resulted in stolen personal information and credit card details for customers and employees. Details regarding the type of virus have not been made public, but the company states that they may receive compensation claims from the affected parties. These cases highlight that in the current maritime threat landscape, not all threats originate from the same geographical location as that of the vessel. This is especially evident in terms of cyberterrorism, whereby threats often do not originate on a vessel and may at times be traced to another part of the world.

3.2 *MS Our Lady of Mediatrix*

On February 25, 2000, multiple bombs exploded on three buses aboard the *MS Our Lady of Mediatrix* ferry that was travelling to Ozamiz City in the Philippines [46]. According to Rubin and Rubin [49], commanders of the Moro Islamic Liberation Front (MILF), which has a significant history of terrorism, were among those blamed for the attack (39-44 killed, 41-50 injured). The explosion of buses onboard the ferry is an example of a successful improvised explosive device (IED) attack, which refers to the use of a “homemade” bomb or destructive device [56]. This case also highlights the threat of using a vehicles-as-a-weapon attack on vessels, as well as on or near excursions. In addition, this case illustrates the use of a fire as a weapon (FAW) [10], whereby the ferry caught fire off the port of Ozamis City as a result of the incendiary bombed rigged to buses on board.

3.3 *MS Achille Lauro*

The most renowned hijacking of a cruise ship took place in October 1985, when the *M.S. Achille Lauro* was seized by four attackers reportedly from the Palestinian Liberation Front (PLF) [21]. The attackers were armed with firearms and grenades that were smuggled on board. Reports at the time by the Italian news agency, ANSA, stated that they did not set out to take control of the ship, but did so after being caught cleaning their weapons by one of the cruise ship’s crew [48]. This raises questions about how the weapons were brought on to the ship and signals the vulnerability that exist for cruise and

passenger ships. The seizure of the ship resulted in the vessel sailing to a number of different ports and countries at the bequest of its captors, with one passenger killed. While the protective security of cruise ships at the time was much different to contemporary approaches, it serves to highlight the potential issues that can arise, particularly if a ship and its passengers are the intended target of terrorist actions.

3.4 *MS City of Poros*

In the morning of July 12, 1988, an explosion killed two men and destroyed a car parked near a marina where the cruise ship *MS City of Poros* was to dock near Athens [18]. This is an example of a failed IED attack, where it is believed terrorists (killed in the explosion) had intended to blow up the cruise ship but were unsuccessful. However, when the targeted ship docked later that evening, attackers stormed the ship with automatic machine guns and grenades, killing nine people and injuring 98. This may also be considered, then, a marauding terrorist attack (MTA) which refers to fast-moving, violent incidents where assailants move through a location aiming to find and kill or injure as many people as possible [11]. In this sense, the attackers began marauding, travelling on foot or in a vehicle, to find and kill or injure more people. This type of challenge includes an armed attack on passengers or crew during boarding, while onboard, during disembarkation, and/or during excursions [4].

3.5 *MV SuperFerry*

On 27th February 2004, the 10,000 ton ‘SuperFerry 14’ left the port of Manila, Philippines, with more than 900 passengers and crew onboard. One hour later, an explosion marked the deadliest terrorist attack at sea ever to date, killing 114 passengers and two crew members [13]. According to the Global Terrorism Database [50], the explosion was caused by a bomb made of eight pounds of TNT, hidden in a TV set onboard the ship, using a watch as a timer. The notorious Abu Sayyaf Group claimed responsibility for the attack. This type of attack is a tragic example of an attack against a passenger ship using an Improvised Explosive Device (IED), as listed in Table 1 with the terrorist threat vectors.

3.6 *MS Carnival Magic*

In 2012, a neurosurgeon, Dr. Jack Kruse, was removed from the cruise ship *MS Carnival Magic* [16] as he was suspected of being armed with biological weapons. The discovery came from a series of tweets posted from a fake Twitter account, posing to be the doctor, which reported that he had brought the Legionnaires virus aboard the Carnival liner with intent to release it. Legionnaire’s disease is a serious type of pneumonia caused by

legionella bacteria [7]. According to the Centers for Disease Control and Prevention (CDC), people can get sick when they breathe in small droplets of water or swallow water containing Legionella. Indeed, legionnaires' disease has been linked to previous deaths of passengers on cruise ships, whereas a man contracted it during a cruise in September 1995 and died 9 days after disembarking [44]. The legionella bacteria from the man were traced back the ship's water supply. Subsequently, another clinically suspected case of legionnaires' disease and one confirmed case were among passengers cruising on the same ship. According to Pastoris et al. (1999), this is the first documented evidence of the involvement of a water supply system in the transmission of legionella infection on ships.

While the case of *MS Carnival Magic* [16] was a false alarm, the incident involving Dr. Kuse highlights the potential for a biological attack on food and water supply of a cruise or passenger ship. To date, passenger vessels have not been subject to bioterrorist attacks [53] but the possibility is real [1]. This may also be considered an insider threat, as Dr. Kruse was set to appear as a guest speaker onboard the Carnival Magic [16]. A principal concern is that of personnel security, and more specifically, insider threat [42]. This relates to workers exploiting their legitimate access to an organisation's assets for unauthorised purposes [12]. An insider could be an employee, a contractor or a business partner; they may deliberately seek to join an organisation to conduct an insider act or may be triggered to act during their employment. Insider threats pose particular risks to the cruise and passenger ship industry. For instance, cruise ships dock in countries with diverse approaches to employee background checks with some employees not undergoing checks at all [57].

4 Assessing Risk of Terrorism for Cruise and Passenger Ships

According to CPNI [9], risks are identified threats aligned to assets, whereby each threat has been assessed for its likelihood of occurring as well as according to the impact that it would have on the organisation and third parties should it transpire. While terrorism is often considered a low-frequency, high-impact security risk, assessing the risks associated with a terrorist attack regularly (at various stages of the cruise ship journey) is key due to both the complexity and large impact associated with such an attack.

4.1 Likelihood

Historically, the world's oceans have not been a major focus of terrorist activity [45]. While this paper differentiates between probable and potential terrorist threats to cruise and passenger ships, the reality is that all threats are low in likelihood. This is due in part to the low frequency of terrorist attacks at sea (as on land). Indeed, some argue that the terrorist risk is

Table 2: Terrorist threat levels to assess likelihood

Threat level	Description
NONE	No indications of a threat. No acknowledged capacity or intent to carry out attacks- unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out attacks- not likely.
MEDIUM	A general threat exists. Capacity and/or intent to attack and possible planning- possible.
HIGH	An acknowledged threat exists. Capacity, intent to attack and planning- likely.
VERY HIGH	A specific threat exists. Capacity, intent, planning and possible execution- very likely.

Source: Adapted from The DDIS [17]

non-existent. For instance, the DDIS consider cyberterrorism threats in 2020-2022 to be “none” [17]. They note that serious cyber attacks aiming to create the effect of conventional terrorism presuppose technical capabilities and organisational resources currently unavailable to militant extremists. In addition, within the given location (Denmark), intention among these groups is limited. However, likelihood can change based on, for instance, where a ship is located. In the context of cruise and passenger ships, whose itinerary may incorporate multiple locations, it is vital to assess likelihood of terrorist threats at each stage of the journey. In terms of likelihood, threat levels (adapted from DDIS) are shown in Table 2.

4.2 Impact

When considering the impact of a potential attack, it is important to note that *“It is not possible to protect everything, so owners and operators must prioritise the highest risk areas of a crowded place”* [14]. Impact may also be experienced outside of the immediate conflict area and may extend to third parties where there is the threat of collateral damage. Therefore, while maritime security tends to focus on impact in terms of scales (low, medium, high), this paper examines impact in terms of wider perceived business risks. Previous research [43] acknowledges various business risks associated with security incidents and highlights the need for decision makers to prioritise them. Parkin et al. (2021) make use of Cambridge taxonomy of Business Risks [6] to assess impact. This taxonomy proposes the following risk types: financial, social, geopolitical, environmental, technology and governance. We choose to look at impact in this way because it breaks down barriers in terms of perception of single risks. For instance, one might assume a cyber-attack carried out by terrorists would pose a technology risk but would be less likely to recognise other associated risks. Financial risk, however, was paramount

in the 2017 cyber attack on Moller-Maersk, the world's largest container shipping line, which brought about \$300 million in direct economic damage and led to a \$8.4 billion loss to shareholders [15]. In this manner, we provide a tool in which decision-makers are prompted to consider a wide spectrum of risks and prioritise them against available resources for response.

A key challenge around impact relates a shift in terrorist targets, from critical infrastructures to crowded places. While both targets may lead to high-impact attacks, attacks on crowded places can be associated with greater impact as harm and loss of life often characterises the most severe attack category (for instance, BIMCO Impact Levels [3]). Thus, emerging terrorist threats have increased significantly in impact- along with the attractiveness of crowded cruise and passenger ships as terrorist targets.

5 Response and Decision-making

Given the unique nature of cruise and passenger ships, this paper envisions a counter terrorism framework to be reviewed at each stop along the vessel itinerary. For that to be done successfully, it must consider limitations to time on those conducting the review, and the fact that these people have other responsibilities as well in their role. Consequently, this framework is designed to inform decision-making and thus improve response to terrorism. Effective protective security response to a terrorist threat should be appropriate, proportionate, timely and coordinated.

An appropriate response to a terrorist threat requires the stakeholders to ensure response is aligned to the risk assessment process. This should be adapted to the ships' circumstances according to the specific stage of the itinerary (considering changes to assets and systems as well as changes to terrorist threats). On the other hand, a proportionate response to a terrorist threat means that the response is only as intrusive as it needs to be to establish an accurate picture of the risks and to neutralise threats. All protective security measures should be proportionate to the level and type of threat [14]. This is especially important for cruise and passenger ships, where tourism companies are focused on customer experience and would not wish to inconvenience customers unless needed.

Responding to a potential terrorist attack also requires a timely and coordinated security response [14]. Regarding coordination, we acknowledge that the cruise ship industry is not responsible nor equipped to counter acts of terrorism alone but should be part of a coordinated response effort. As listed in Australia's Strategy for Protecting Crowded Places from Terrorism [14] "*Countering terrorism is a responsibility shared by all Australian governments, the community, and the private sector.*" Thus, the proposed framework aims to offer guidance for cruise ships to manage terrorism risks by means of a strategic response that is underpinned by effective decision-making.

6 Evaluation

Once an organisation responds to a terrorist threat, invariably there are opportunities to improve future response. Evaluations of incidents are critical to improvements, the conclusions of which should be fed back into the planning process. Such evaluations should consider lessons learned, effectivity, and consequences (intended/unintended).

Incorporating lessons learned into future response preserves the relevance of a framework over time, as it not only allows continuous improvement of the framework but also ensures being able to respond to new and evolving threats. Experience and expertise of management must continue to develop over time as new threats emerge [40]. This speaks to resilience as it implies *“not the presumption of sufficient knowledge, but the recognition of our ignorance; not the assumption that future events are expected, but that they will be unexpected”* [22]. This too incorporates an element of creativity, *“most important in the context of social resilience and national security,”* where it’s not about returning to an initial equilibrium, but rather adapting to new circumstances and learning from experience [5].

Evaluation of response should be effective, which requires measures of effectivity. While this research conceptualises a strategic counter terrorism framework for cruise and passenger ships, and recognises the need to develop performance measurement tools, it does not propose such tools. This is because tools for effectivity should be considered after the framework is operationalised.

Finally, evaluation of response should also consider consequences, both intended and otherwise. Relevant here is the idea of *“bouncing forward”* [47] from external shocks (consequences) which may be seen as offering a more radical framework within which the opportunities for local innovation and creativity can be assessed and explained. To be effective, tools must reflect strategies that are *“continuously changing and capable of mutation”* [37]. Thus, higher levels of functioning and resilience are attained.

7 A Counter Terrorism Framework for Cruise Ships

This research proposes a framework that conceptualises the protection of the cruise and passenger ships from terrorism, as presented in Figure 2. To develop this framework, inspiration was taken from the protective security risk management model proposed by CPNI [9]. In response to the multi-stage itinerary, it is purposefully intended that the framework is not inhibited by location and instead can act as a consistent approach to protective security for any city and country.

The proposed framework first considers the registry of the vessel, as the principal legal and testing responsibilities mainly lie with the vessel including the ship’s flag state. Although such a vessel may traverse multiple locations during its journey, this research argues that the core components of protective

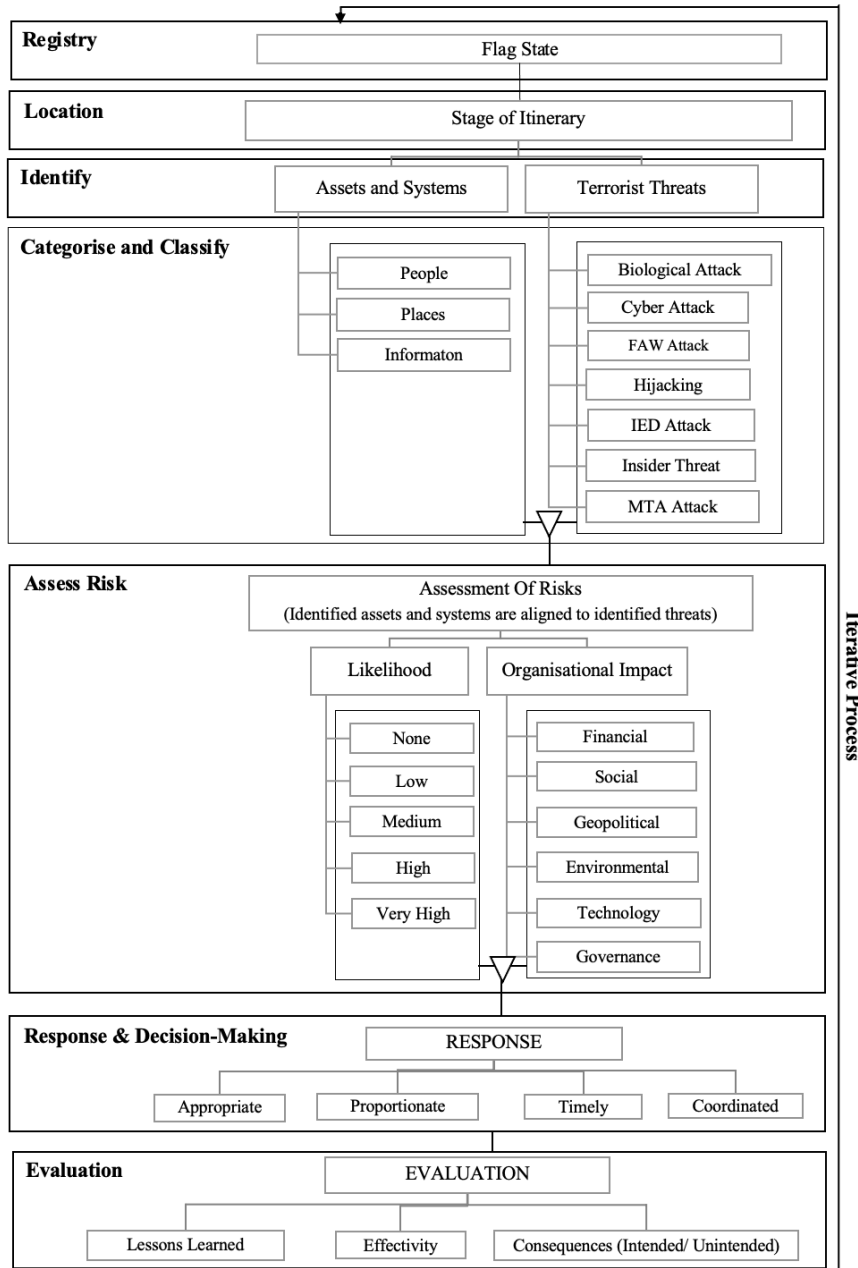


Fig. 2: Counter Terrorism Framework for Cruise and Passenger Ships

security are transferable, even if the lead actor for implementation may differ by location and have different capability levels in terms of delivery. This is because the vessel itself remains relatively unchanged in its strategic needs at sea and in port regardless of location. Thus, the framework is designed to be used at each stage of the cruise ship itinerary.

At each stage in the itinerary, we then examine the components of protective security for cruise and passenger ships presented in Section 2 to identify core assets and systems that need to be protected. These systems and assets can be categorised in relation to their level of criticality in supporting business. They may then be classified according to the amount of potential damage their compromise would cause to the organisation [8]. Secondly, we identify the terrorist threats to the cruise ship industry, which relate to those identified in Section 3. We then explore how identified assets and systems align with identified threats, to inform risk assessment. Each risk is assessed in terms of their likelihood to transpire and the impact such an occurrence would have to the organisation or third parties, as outlined in Section 4. This allows risks to be prioritised in terms of strategic response, outlined in Section 5, which is underpinned by effective decision-making that is appropriate, proportionate, timely and coordinated. Finally, following response, the incident is evaluated according to lessons learned, effectivity and consequences (intended and unintended) to ensure continuous improvement and the ability to respond to new and evolving terrorist threats, as discussed in Section 6.

8 Conclusion

In the present context of global terrorism, managing terrorist risks in cruise and passenger ships is a challenge for organisations. This paper evidences that terrorists have targeted such vessels previously and argues that there are a range of terrorist threats that collectively result in a complex and dynamic risk environment that is unique to the industry. To address this challenge, this paper conceptualises a counter terrorism framework for cruise and passenger ships. This framework draws upon key components of protective security, as well as terrorist threats which are informed by known attacks on cruise and passenger ships. It includes a method to assess risk at each stage of the ship's journey, which in turn provides a means for industry stakeholders to identify and counter terrorist threats. In this way, this research offers a consistent approach to delivering an effective protective security posture at all stages of a ship's itinerary. It is envisaged that the application of the framework will improve security decision-making within organisations which, over time, has the potential to enhance deterrence.

Looking forward, it is important that the framework is trialled in different contexts to ensure it is transferable. Further, industry stakeholders should be engaged in ways that are sensitive to their interests, needs and

capabilities. In this way, the framework can be validated and then operationalised by industry stakeholders, at which point measures of effectivity can be established to guide evaluation. We aspire that this framework, once validated, may be sit alongside existing requirements on vessels and ports that stem from regulatory frameworks such as the ISPS Code [25]. Emphasis needs to be placed on laying out the benefits of recognising core components to protective security for added consistency, whilst keeping open the space for sharing experiences and innovation in relation to specific policies and practices implemented. Here, more work is needed to bring together land and maritime focused practitioners, the public and private sector, and to explore any grey areas brought about by questions of jurisdiction and maritime law. For researchers interested in this subject, refinement of this framework through its deployment in relation to different cruise and passenger ship routes globally, where varied protective security governance exist, is a clear avenue for future research.

References

1. Nic Robertson, Paul Cruickshank and Tim Lister, CNN: Documents reveal al Qaeda's plans for seizing cruise ships, carnage in Europe (2012). <https://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/index.html>
2. Ahmad, M.: Maritime piracy operations: Some legal issues. *Journal of International Maritime Safety, Environmental Affairs, and Shipping* 4(3), 62–69 (2020)
3. BIMCO: The Guidelines on Cyber Security Onboard Ships- Version 3 (2018)
4. Bowen, C., Fidgeon, P., Page, S.J.: Maritime tourism and terrorism: Customer perceptions of the potential terrorist threat to cruise shipping. *Current issues in tourism* 17(7), 610–639 (2014)
5. Briggs, R.: Building strong communities to tackle the terror threat. paper presented at BISA Annual Conference, Exeter University, 15–17 December 2008 (2008)
6. Cambridge Centre for Risk Studies: Global Risk Index 2020: Executive Summary (2019)
7. Centers for Disease Control and Prevention (CDC): Legionella (Legionnaires' Disease and Pontiac Fever) (2021). <https://www.cdc.gov/legionella/index.html>
8. Centre for the Protection of National Infrastructure: Advice & Guidance (2018). URL <https://www.cpni.gov.uk/advice-guidance>
9. Centre for the Protection of National Infrastructure: Protective Security Risk Management (2019). URL <https://www.cpni.gov.uk/rmm/protective-security-risk-management>
10. Centre for the Protection of National Infrastructure: Fire as a Weapon (2021). URL <https://www.cpni.gov.uk/fire-weapon-0>
11. Centre for the Protection of National Infrastructure: Marauding Terrorist Attacks (2021). URL <https://www.cpni.gov.uk/marauding-terrorist-attacks-1>
12. Centre for the Protection of National Infrastructure: Reducing Insider Risk (2021). URL <https://www.cpni.gov.uk/reducing-insider-risk>
13. Chapsos, I., Noortmann, M.: Maritime terrorism. In: *The SAGE Encyclopedia of Political Behaviour*, pp. 462–463. SAGE Publications (2017)
14. Commonwealth of Australia: Australia's Strategy for Protecting Crowded Places from Terrorism (2017). URL <https://www.nationalsecurity.gov.au/crowded-places-subsite/Files/australias-strategy-protecting-crowded-places-terrorism.pdf>
15. Cyberhedge: World's second largest container shipping company msc suffers a network outage, possibly due to a cyber attack (2020). URL <https://cyberhedge.com/insights/daily/2020/04/14/world-s-second-largest-container-shipping-company-msc-suffers-a-network-outage-possibly-due-to-a-cyber-attack/>

16. Daily Mail: Neurosurgeon ordered off cruise after fake Twitter account said he planned on staging 'epic' bio-terrorist attack (2012). <https://www.dailymail.co.uk/news/article-2142006/Neurosurgeon-pulled-cruise-fake-bio-terrorism-Tweet.html>
17. Danish Defence Intelligence Service: The cyber threat against the danish maritime industry and ports (2020). <https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/cfcs-cyber-threat-danish-maritime-industry-and-ports-.pdf>
18. Dopoulos, P.: URGENT Gunmen Fire Aboard Cruise Ship; 9 Killed, 98 Wounded (1988). URL <https://apnews.com/article/c7e8b81dc7192ad34b0e123a5f11cd4e>
19. Gathii, J.T.: Kenya's piracy prosecutions. *American Journal of International Law* **104**(3), 416–436 (2010)
20. Halberstam, M.: Terrorism on the high seas: the achille lauro, piracy and the imo convention on maritime safety. *American Journal of International Law* **82**(2), 269–310 (1988)
21. Heathcote, P.: An explanation of the new measures for maritime security aboard ships and in port facilities. *Maritime Studies* **2004**(137), 13–21 (2004)
22. Holling, C.S.: Resilience and stability of ecological systems. *Annual review of ecology and systematics* **4**(1), 1–23 (1973)
23. IMO: Msc-fal.1/circ.3 guidelines on maritime cyber risk management (2017). URL [https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20\(Secretariat\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf) [Online; accessed 15-July-2021]
24. International Maritime Organisation: Resolution MSC.428 (98) Maritime Cyber Risk Management in Safety Management Systems IMO Doc. MSC 98/23/Add.1, Annex 10 (2017). URL [https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428\(98\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf)
25. International Maritime Organization: ISPS Code: International Ship and Port Facility Security Code and SOLAS Amendments 2002 (IMO: London) (2003). URL <https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx>
26. International Maritime Organization: Strategy for the development and implementation of e-navigation (2019). URL <http://www.imo.org/en/OurWork/Safety/Navigation/Pages/eNavigation.aspx>
27. Joyner, C.C.: Suppression of terrorism on the high seas: The 1988 imo convention on the safety of maritime navigation. In: *Israel Yearbook on Human Rights*, Volume 19 (1989), pp. 343–369. Brill Nijhoff (1989)
28. Karim, M.S.: The international law of maritime terrorism. In: *Maritime Terrorism and the Role of Judicial Institutions in the International Legal Order*, pp. 39–66. Brill Nijhoff (2017)
29. Karim, M.S.: Maritime cybersecurity and the imo legal instruments: Sluggish response to an escalating threat? *Marine Policy* **143**, 105138 (2022)
30. Kipkech, J., Kuhn, K. & Shaikh, S.: *Cyber Security and Disruptive Technologies*, chap. 21. Routledge Handbook of Maritime Security (2021)
31. Korff, D.: The territorial (and extra-territorial) application of the gdpr with particular attention to groups of companies including non-eu companies and to companies and groups of companies that offer software-as-a-service. Available at SSRN 3439293 (2019)
32. Kuhn, K., Bicakci, S., Shaikh, S.A.: Covid-19 digitization in maritime: understanding cyber risks. *WMU Journal of Maritime Affairs* **20**(2), 193–214 (2021)
33. Malcolm, J.A.: Project argus and the resilient citizen. *Politics* **33**(4), 311–321 (2013)
34. Malcolm, J.A.: Responding to international terrorism: the securitisation of the united kingdom's ports. *The British journal of politics and international relations* **18**(2), 443–462 (2016)
35. Maritime Executive: Carnival Corporation Reports Ransomware Attack Accessed Data (2020). <https://www.maritime-executive.com/article/carnival-corporation-reports-ransomware-attack-accessed-data>
36. McIlhatton, D., Berry, J., Chapman, D., Christensen, P.H., Cuddihy, J., Monaghan, R., Range, D.: Protecting crowded places from terrorism: an analysis of the current considerations and barriers inhibiting the adoption of counterterrorism protective security measures. *Studies in Conflict & Terrorism* **43**(9), 753–774 (2020)

37. McKee, K.: Post-foucauldian governmentality: What does it offer critical social policy analysis? *Critical social policy* **29**(3), 474 (2009)
38. Mensah, T.A.: The place of the isps code in the legal international regime. *WMU Journal of Maritime Affairs* **3**(1), 17–30 (2004)
39. National Counter Terrorism Security Office: Crowded places guidance (2020). URL <https://www.gov.uk/government/publications/crowded-places-guidance>
40. O'Brien, G., Read, P.: Future uk emergency management: new wine, old skin? *Disaster Prevention and Management: An International Journal* (2005)
41. OJ L 119: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016). URL <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
42. Orosz, M.D., Southwell, C., Barrett, A., Bakir, O., Chen, J., Maya, I.: Portsec: Port security risk management and resource allocation system. *IFAC Proceedings Volumes* **42**(15), 135–142 (2009)
43. Parkin, S., Kuhn, K., Shaikh, S.A.: Scenario-driven assessment of cyber risk perception at the security executive level. In: *Workshop on Usable Security and Privacy*, pp. In-Press (2021)
44. Pastoris, M.C., Monaco, R.L., Goldoni, P., Mentore, B., Balestra, G., Ciceroni, L.: Legionnaires' disease on a cruise ship linked to the water supply system: clinical and public health implications. *Clinical Infectious Diseases* **28**(1), 33–38 (1999)
45. Peter Chalk, RAND Corporation: The maritime dimension of international security: Terrorism, piracy, and challenges for the united states (2008). URL <https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND.MG697.pdf>
46. Rubin, B., Rubin, J.C.: *Chronologies of modern terrorism*. Routledge, New York (2008)
47. Shaw, K.: The rise of the resilient local authority? *Local Government Studies* **38**(3), 281–300 (2012)
48. Smith, W.E.: *Terrorism: The voyage of the achille lauro* (1985)
49. Stanford University: Mapping Militant Organizations. "Moro Islamic Liberation Front." (2019). URL <https://cisac.fsi.stanford.edu/mappingmilitants/profiles/moro-islamic-liberation-front#text.block.20203>
50. START (National Consortium for the Study of Terrorism and Responses to Terrorism): Global Terrorism Database 1970 - 2020 [data file] (2020). URL <https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=200402270002>
51. Stewart, M.G., Mueller, J.: Aviation security, risk assessment, and risk aversion for public decisionmaking. *Journal of Policy Analysis and Management* **32**(3), 615–633 (2013)
52. The American Club: Piracy – Frequently Asked Questions (FAQs) (2009). URL https://www.american-club.com/files/files/MA_Piracy_faq_060209.pdf
53. Tran, M.: Lost at sea-plunge into cruise ship jurisdiction: Which governmental agency regulates health on passenger vessels, which governmental agency responds in the event of a biological attack on a vessel, and what can be done to prepare. *J. Biosecurity Biosafety & Biodefense L.* **6**, 109 (2015)
54. UN General Assembly: United Nations Convention on the Law of the Sea, Article 101 (1982). URL https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf
55. U.S. Coast Guard, I.P.S.P.: Security threats and trends (2019). URL https://portalcip.org/wp-content/uploads/2019/08/8-Security-Threats-and-Trends_May19.pdf
56. U.S. Department of Homeland Security and The National Academies: IED Attack: Improvised Explosive Devices (2021). URL https://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf
57. Walker, C.M.: Cruise ships: The next terrorism target. *Travel Law Quarterly* **2**, 124–135 (2012)
58. Wambua, M.: A critical review of the global legal framework on piracy: 40 years after unclos. *Maritime Affairs: Journal of the National Maritime Foundation of India* **18**(1), 134–148 (2022)