COVID-19 digitization in maritime: understanding cyber risks

Kuhn, K., Bicakci, S. & Shaikh, S.

Original citation & hyperlink:
Kuhn, K, Bicakci, S & Shaikh, S 2021, 'COVID-19 digitization in maritime: understanding cyber risks', WMU Journal of Maritime Affairs, vol. 20, pp. 193-214. https://doi.org/10.1007/s13437-021-00235-1

DOI https://doi.org/10.1007/s13437-021-00235-1
ISSN 1651-436X
ESSN 1654-1642

Publisher: Springer

The final publication is available at Springer via http://dx.doi.org/10.1007/s13437-021-00235-1

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

Decoding COVID-19: Digital Acceleration and its Implications for Maritime Cybersecurity

Case Study: NATO Collective Cyber Risk Perception

Kristen Kuhn[1] · **Salih Bicakci**[2] · **Siraj Ahmed Shaikh**[13]

the date of receipt and acceptance should be inserted later

Abstract COVID-19 hastens a digital acceleration which has wide implications for maritime cybersecurity. The global shipping industry relies heavily (and increasingly) on technologies which do not ship vulnerability free. Cyber attacks on these technologies can cripple critical systems and services, for extended time and at significant cost. Consider the destabilising ransomware attacks upon shipping giants Maersk [11] and CMA CGM [39]. Such incidents motivate stakeholders in the sector to engage with cyber risks. Our contribution explores cyber risk perception through the development of a structured, scenario-driven and repeatable exercise for decision-makers. The exercise was delivered at a NATO Centre of Excellency to raise awareness, but it also offers insights on how to assess cyber risk perceptions of a group– and how perception impacts response. Our findings highlight the essential need to plan for cyberspace operations and lay a foundation for cyber risk perception as a intricate governing factor in maritime.

Keywords Cybersecurity · Cyber risk management · Decision-making · Maritime · Risk perception

1 Introduction

In October 2020, the International Maritime Organisation (IMO) tweeted: "The interruption of service was caused by a cyber attack against our IT systems" [31]. This attack had serious implications, coming at a time when the IMO was under intense scrutiny, working to bring attention to the global

[1]Systems Security Group, Institute for Future Transport and Cities, Coventry University, Coventry CV1 5FB, United Kingdom
[2] Department of International Relations, Kadir Has University, Turkey
[3]Security, Risks Management and Conflict (SEGERICO) Research Group, Universidad Nebrija, 28015, Spain

crew crisis, and- ironically- asking its member nations to enforce IMO 2021, a resolution requiring ship owners to invest in cybersecurity [19].

The IMO was the second major shipping organisation to be hit by a cyber attack that week, and the fifth high-profile attack in 2020 [46]. It came three days after Shipping Giant CMA CGM reported a ransomware attack [39]. The logistics company Toll Group was also hit by two distinct ransomware attacks, in January and in May [33]. Mediterranean Shipping Company (MSC) suffered a malware attack at its Geneva headquarters in April [47]. Cybersecurity experts suggest the surge in attacks this year results from distractions and increased reliance on digital services due to COVID-19 [46].

The global COVID-19 lockdown of 2020 disrupted the world economy. It led to a rapid uptake of digital communications and trade that will have a lasting impact, and which comes with an increase in cyber risk. This is no more vivid than in the maritime sector, where the global shipping industry relies heavily (and increasingly) on technologies that do not ship vulnerability free. Understanding maritime cyber risk is a challenge because it is a complex and evolving risk that affects trade, geopolitics, and security. We explore cyber risk management and, in particular, why cyber risk perception is a key factor but also a difficult one to grasp. We also outline the implications of these, and the push for digital technologies, on maritime cybersecurity.

In June 2020, The North Atlantic Treaty Organization (NATO) issued a statement [30] condemning cyber-attacks inflicted amidst the ongoing global health pandemic. NATO, a collective leadership body that extends to the maritime domain, must address COVID-19 and its cybersecurity significance. Yet, some argue its partners lack a shared situational awareness on cyber threats [21] which could hinder collective response. This has much to do with risk perception. In this context, our research is motivated by the question: How can cyber risk perception be assessed effectively? Further, does work experience and cybersecurity expertise affect incident response?

To address these questions, we develop a cybersecurity decision-making game, which was conducted at a 2020 NATO training course at The Centre of Excellence Defence against Terrorism (COE-DAT). Using scenarios that range over distinct cyber incidents in the maritime domain, we examine the cyber risk perception of a group of 68 participants from 29 states. This group had significant military/ public sector experience and varied cybersecurity expertise. Effective assessment of cyber risk perception was done by calibrating risk in a group setting. Results indicate that as incident impact rose, group response favored private sector responsibility and visibility, but not urgency or directness. From this, we explore collective risk perception- tendencies which characterise NATO security culture. We then discuss implications for practice, with special care to interpret findings in the context of the ongoing COVID-19 pandemic. Our approach demonstrates collective risk perception is a key aspect of proactive decision-making, and can be not only measured, but improved significantly through iterative learning.

1.1 Our contribution

This exercise is a capacity building tool for maritime organisations, trialled successfully in small setting. It fosters preparing for secure use of cyberspace in the maritime environment. Further, it addresses a key disconnect in crisis response, by sharpening technological skills and decision-making, when "NATO table-top exercises at the political strategic level are not sufficiently linked to the technical cyber level" [21]. We offer insights into how such exercises can build capacity and the need for joint response.

While the exercise was delivered during at a training course at COE-DAT as a tool to raise awareness, it also led to insights on how to assess the cyber risk perception of a group– and how these perceptions impact the nature of response. Our findings highlight the importance of planning for cyberspace operations and lay a foundation for cyber risk perception as a intricate governing factor in maritime.

The rest of this paper is organised as follows: Section 2 includes background information. Section 3 introduces NATO as a case study and explores its collective cyber risk perception. Section 4 presents our methodology. Section 5 displays results and Section 6 includes a discussion of these results, including their relevance to the ongoing COVID-19 pandemic. Section 7 outlines our conclusions.

2 Background

2.1 Digital acceleration and implications for maritime cybersecurity

The global COVID-19 lockdown of 2020 disrupted the world economy. Four billion people (51 per cent of the world's population) were locked down by government mandate in the first half of the year [5]. Citizens were unable to work, visit shops, travel or socialise. This lockdown led to a 4 per cent reduction in global GDP [22] and resulted in over $5 trillion of output lost in six months [45]. However, more than a restriction, the COVID-19 crisis has transformed how we do work, trade, and crime; and the way these will continue to be done in the future. The amount of the economy that is now reliant on IT systems has increased significantly and as a sudden spike [5].

The looming pandemic has many researchers investigating just how much digital change COVID-19 has caused organisations [32]. Most results show that digitisation has increased significantly [5] and that (as a result) cyber crime is on the rise [26]. Rapid societal transformations experienced during the outbreak, which have increased the frequency and variety of online activity, have created new opportunity structures [20]- both legitimate and otherwise.

2.1.1 Legitimate digital opportunity structures that increase cyber risk

Increased internet use is associated with legitimate opportunities for business from offline to online environments. For instance, due to COVID-19, global e-

commerce sales grew by 207 per cent in April 2020 alone [52]. During lockdown, online shopping reached mammoth proportions, as new and existing online consumers seek to obtain products via available means [1].

Remote working is another new opportunity for many. Using platforms such as Microsoft Teams and Zoom, COVID-19 has rapidly propelled many industries that have been able to continue operating to work remotely without offices [1]. According to Ido Ben-Moshe, Vice President of Business Development for maritime cybersecurity company Naval Dome, remote working and an increase in remotely controlled, autonomous technologies will likely accelerate during and after COVID-19 [46].

Navigating the new world in terms of online trade and remote working is not without its challenges. While digitisation fosters business opportunities, it adds complexity to security protection and makes organisations' systems more valuable. Disinformation and poor employee security awareness in these new conditions has compounded this problem [5]. According to Ido Ben-Moshe, "This will see companies face new cyber security challenges if they fail to implement adequate protective measures" [46]. Jamie Akthar, CEO and Co-founder at London-based cybersecurity firm CyberSmart adds: "Equipping employees with the skills they need to prevent breaches is absolutely essential for businesses today, particularly as they transition into a work environment that is increasingly online" [10]. While Akthar is correct, most cyber incidents are outcomes of human error- or they are exploited by accident, it is worth mention that cybercrime is also on the rise.

2.1.2 Illegitimate digital opportunity structures that increase cyber risk

Increased internet use is also accompanied by a shift in illegitimate opportunities, like crime, from offline to online environments [26]. Early research [20] found the amount of cyber-attacks reported globally increased during the COVID-19 outbreak. And while the implications of COVID-19 are still being understood, it's safe to assume a bump in all areas of cyber crime [43]. That is, increased digitisation brings increased cyber risk. Buil-Gil et al. [3] suggests cyber crime increased during the pandemic, at rates especially high during months with strict lockdown policies. In particular, they note the largest increase in the number of online fraud incidents associated with online shopping and auctions, and the hacking of social media and email. Collier et al. [6] observe increased denial of service attacks , and Colburn [5] points to increases in ransomware attacks and in the activity of state-sponsored groups stemming from geopolitical tensions.

Rising cybercrime and cyber-attack rates are also observed in the maritime sector. The 2020 Maritime Cybersecurity Survey by Safety at Sea and BIMCO found almost a third of maritime organisations experienced cyberattacks- a 9 per cent increase from the previous year [24]. Akin to Buil-Gil et al. [3], this study also identified fraud as the main cyber incident in the maritime sector, including phishing (68 per cent of attacks) and spear phishing (41 per cent). Malware was the third most common incident (33 per cent).

2.1.3 Implication for maritime cybersecurity

All of these digital opportunity structures, legitimate and illegitimate, have direct implications for maritime cybersecurity. The use of new technology adds critical cyber risk elements, where vulnerable systems in place to support operations increase cyber risk by expanding attack surface. If detected by an adversary, these systems can be exploited and used to exacerbate impact. Not only does the technology surge make cyber attacks easier to perform, but increased success rates make them more lucrative. The expansion in exposure to cyber risk has attracted a proliferation in threat actors and attack technology [5]. Thus, COVID-19 has driven a major increase in cyber risk.

Indeed, the pandemic has especially wide implications for the maritime sector, where the global shipping industry relies heavily (and increasingly) on technologies that do not ship vulnerability free. For instance, in today's digital-first environment, customers depend on "just in time" (JIT) supply chains to track business links with partner companies [7] and shipped goods. JIT saves a lot of money because there is less spent on holding things in stock, but creates vulnerabilities if shipments are delayed or lost [43]. Operational shutdowns, which may be consequence to cyber-attacks, can cause costly disruptions that quickly ripple through vulnerable systems and networks [7]. Currently, these supply chains are badly stretched due to COVID-19, adding immense pressure on organisations to quickly restore any loss of control of IT systems and resume normal operations. This was the case for MSC, who fell victim to a cyber-attack in April 2020 [47], where clients had to resort to secondary communication means-via phone, email or through local offices- to contact the company in the aftermath of the attack.

Looking back, digitisation was a growing factor in shipping before COVID-19, making cybersecurity increasingly relevant. One only needs recall the 2017 Not-Peta ransomware attack on Moller-Maersk, which disrupted their operations for two weeks, resulted in a 20 per cent reduction in shipping volume during the outage, caused $300 million in direct economic damage and led to $8.4 billion in value loss to shareholders [7]. This attack has driven the importance of cybersecurity home for many, and has since become a notorious, almost legendary cyberattack in maritime. Organisations can can ill afford to deal with cyber attack-driven operational disruption such as that faced by Maersk in 2017. However, this is not the only high profile cyber attack to hit the maritime industry since then; eight from the past two years alone are listed in Table 1.

Looking forward, the maritime industry continues to expand; In the year preceding the pandemic, the ITF Transport Outlook 2019 predicted maritime freight transport will grow at a compound annual rate of 3.6 per cent through 2050, and that maritime trade volumes will almost triple [17]. Cyber risks also increases on this trajectory. COVID-19, and greater reliance on digital, has accelerated these trends and held a magnifying glass to the issue.

Table 1: Survey of eight recent cyber-attacks in the maritime industry, including the date (month/year), target, and a brief description of the attack.

Date	**Target**	**Description**
10/20	IMO	Malware attack that disabled their website and intranet, forcing the UN organisation to shut down key systems to prevent further damage [19].
09/20	CMA CGM	Ransomware attack on its Chinese offices, forcing the container line to shut down its network and many online services to prevent further damage [39].
09/20	US tug boat	Phishing attack involving a malware email which spoofed the vessel operator, who sent it to the vessel via an Office 365 voicemail attachment, then notified authorities. [10].
01/20	Toll Group	Ransomware attack using 'Netwalker' software that hit land and sea operations. They shut down systems, caused delays and disruptions, attributed to Russian hackers [33].
04/20	MSC	Malware attack that caused network outage that affected systems at the shipping line's Geneva headquarters, resulting in disruption but minimal damage [47].
06/20	Toll Group	Ransomware attack using 'Nefilim' software, which led to stolen personal and business information and caused the shut down of IT systems to prevent further damage [33].
06/20	Shahid Rajaee Port	Malware attack on Iranian port on the Strait of Hormuz that crashed the facility computer system and caused transport chaos for days, attributed to Israel [28].
07/19	*Stena Impero*	GPS spoofing of a UK tanker that sent it off course as it entered the Strait of Hormuz where Iran seized ship and its 23 crew, attributed to Iran [50].

2.2 Understanding maritime cyber risk

International shipping facilitates around 90 per cent of world trade [16] and is an $183.3 billion industry [44]. It fosters intercontinental exchange; the bulk transport of raw materials, and the import/export of food and manufactured goods. The maritime realm is also critical for defense and has geopolitical importance. Consider the highly contended and lengthy dispute over the South China Sea, where geopolitical considerations include not only sovereignty, but access to energy reserves, critical sea lanes, marine living resources and the environment, as well as ever evolving military and strategic aims [37]. This example, known as the 'doughnut hole,' encompasses a geographic area smaller than each of the five oceans. In context, it is hard to imagine a more valuable target than the maritime realm, its ships and networks.

Whether deliberate or accidental, maritime cybersecurity incidents can have catastrophic consequences. "With such interconnected operations, one breach within one company in a supply chain can have serious knock-on effects for the other suppliers or organisations they work with," says Jamie

Akthar, CEO and co-founder at CyberSmart [10]. Envision the "unimaginable" damage that would occur if hackers entered into the autopilot systems of an entire global fleet of vessels [19]. Consider also the damage associated with a cyber-attack in which a computer virus infects 15 major ports across Asia Pacific, a scenario developed in 2019 which estimates economic loss upwards of $110 billion [34].

Maritime cybersecurity incidents can take many forms. Areas of marine cyber risk include physical damage, loss of availability and extortion [23]. Incidents can affect vessels, shore-side operations, and in-between. Cyber risks to vessels includes physical damage (e.g. running aground, collision) or loss of hire (e.g. not seaworthy, systems not operating or ransomed). Shore-side cyber risks include bricking (e.g. computer hardware onshore), business interruption or data loss, (e.g. Onshore systems fail or ransomed).

Cybersecurity incidents may result in breached data/privacy/saftey, delay or disruption, and various types of business risks [35] (e.g. financial, geopolitical, environmental and social; technology and governance). Here, *risk* involves a state of uncertainty where some of the possibilities involve a loss, injury, catastrophe, or other undesirable outcome [13]. Understanding maritime cyber risk is a challenge as it is complex, evolving, and asymmetrical [8]; larger attack surfaces and greater uncertainty makes it hard to assess risk and formulate response. Accelerated digitisation, a result of COVID-19, is associated with increased cyber risk and that means less time for organisations to prepare response. While cyber incidents are inevitable, and risk cannot be eliminated, it must be managed.

2.2.1 Cyber risk management in the maritime sector

As cyber incidents are inevitable, risk strategy for maritime organisations should include preparedness. The varied nature of cyber threats means there is no single approach to address all resulting risks. The rate of technology change and the steady flow of serious vulnerabilities in operating systems, software libraries and applications means that any strategy must be regularly reviewed. Organisations must consult guidelines, consider risks, and take stock of their capabilities to gauge their level of cyber readiness.

Cyber risks are here to stay and prudent maritime organisations should consider how best to manage these risks. Aforementioned, the IMO is launching new cybersecurity guidelines in that require shipping to beef up digital security measures by the end of 2020 [19]. The United States Coastguard, BIMCO and the International Chamber of Shipping have also recently released cybersecurity guidance for ship owners [53]. A 2019 study [42] develops a streamlined framework to assess cyber risks on ships, which includes sector relevant guidelines, like those established by BIMCO [2]. Yet, "despite the heightened focus by regulators and industry bodies on the risks posed by cyber, more progress is needed" [53].

A key component of cyber risk management is discerning who owns cyber risk, in terms of best practices, operations and investments. Cybersecurity

cannot be addressed through technology alone, and often requires strategic response from decision-makers [15] who must also rely on their own risk perception. Corporate boards and company directors, who have the ultimate ownership for effective risk management, are under increasing pressure to be more transparent on the state of preparedness to respond to cyber-attacks.

Even if ownership and guidelines are clear, an organisation's risk appetite- what they are willing to invest in cybersecurity- is often not. Alongside digital acceleration, increased cyber risk is linked to COVID-19 because it encourages organisations to place cyber risk on the back burner. The global lockdown has led to a shift in the perception of business leaders, from a longer-term to short-term outlook- or survival. Jamie Akthar, CEO and co-founder at CyberSmart explains: "Cybercriminals are opportunistic and we have seen a rise in breaches since the pandemic because they know most industries are directing their attention to keeping business operations afloat rather than investing in security" [10]. Despite increased cyber risk, daily operations and resiliency trumps strategic aims and investment, where cybersecurity kicks its heels.

2.2.2 Cyber risk perception in the maritime sector

Risk perception is relevant to leaders because it influences their decision-making. It is acknowledged that, among other factors, perception rests on a foundation of experience [36]. Those who have not responded to a previous cyber-attack of similar nature have little reference, which is a contributing factor to poor performance. Subjectivity is another key challenge as risk is often formed on the basis of perception. *Perceived risk* is the estimated likelihood of occurrence [36], be it negative or positive. Indeed, these two aspects – positive and negative – make risky choice play a central role in decision-making under uncertainty [38].

One way to learn about perceived risk is to look at response, either to actual or hypothetical events. For instance, a 2019 study [40] proposes a virtual environment to observe egress skills on offshore petroleum platforms. Likewise, the exercise-based approach used in this study is demonstrated [18] to improve incident response through iterative learning. Errors in judgement, often due to incorrect risk perception, can lead to disproportionate response, such as mistakes in saftey, resource allocation or incident escalation. In other words, gaps in perception of risk indicate gaps in capabilities to act [51].

Rather than the researcher being an expert, we assume our participants are the experts in the room since many work in professions where they are tasked to respond to cyber incidents. We work with an expert group, then, to learn about their collective cyber risk perception. An advantage, unique to working with experienced or expert decision-makers, is the idea of using an exercise to calibrate the group. That is, while exercises played by individuals aim at capacity building, exercises played by groups can also aim at communication and thus offer an internal qualitative measurement system. This is especially relevant when working with groups of participants that have a wide range of

backgrounds, e.g. work experience, cybersecurity expertise. This impacts risk perception: "Risk, after all, is a matter of perception and every society has not only a different perception of risk, but also a different threshold for risk" [51].

This study includes 68 participants with varied levels of cyber expertise. It is a unique sample group that has its own risk culture, perception and threshold. We explore participant backgrounds to learn why they might respond as they do to cyber incidents. While there is no right or wrong response, calibrated responses indicate effective assessment and streamlined risk perception.

3 Case Study: NATO collective cyber risk perception

In June 2020, NATO issued a statement [30] condemning cyber-attacks inflicted amidst the COVID-19 pandemic. About a month later, the UK National Cyber Security Centre warned that Russia's APT29, a cyber threat actor known as "Cozy Bear," targeted COVID-19 vaccine researchers [27]. Their assessment was supported by key allies, including the Canadian Communication Security Establishment and the US National Security Agency.

Whereas one of the first steps of cyber incident response is to recognise an attack, NATO served as a collective body to communicate information- over a month before its partners did so independently. This is an active demonstration of NATO's three core tasks, as defined in the 2010 Strategic Concept [29]: collective defense, crisis management and cooperative security. It also outlines the big achievement of NATO: collective response.

It's not always that easy. The complexities of cybersecurity are a key factor in cyber incident response. Credible deterrence in cyberspace depends on capacity and readiness to respond to cyber incidents. While it is individual states who decide to act, collective response is possible among states that share similar risk perception and a willingness to respond. By aligning to NATO, member states can cultivate a group risk culture and agree to support group response. However, this can be problematic when not all partners agree on cyber threats.

With respect to maritime cyber operations, a starting point for effective incident response is to streamline cyber threats. Today, there is little to suggest shared situational awareness on cyber threats across NATO partners [21]. This has much to do with risk perception. In this context, our research is motivated by this first question: How can cyber risk perception be assessed effectively? To address this, we developed a cybersecurity decision-making exercise, which was conducted at a 2020 NATO training course at COE-DAT.

Cyber risk perception and proportionate response to cyber attacks are critical capabilities for NATO partners. Assessing collective perception is a challenge, particularly when individual capacity and level of preparedness is variable. Our cybersecurity decision-making exercise is a tool to foster capacity building and improve understanding of maritime cybersecurity.

3.1 The Centre of Excellence Defence against Terrorism

This Centre of Excellence Defence against Terrorism (COE-DAT) is one the oldest NATO centers, inaugurated in 2005. It is composed of eight representatives from various nations to advise on field-proven solutions and to challenge decision-makers on terrorism and counter terrorism. COE-DAT acts to harmonize NATO resources and serves as the NATO Department Head in Education and Training. It also presents a prospective outlook for the transformation of terrorism and its association with future security challenges to collective defense and cooperative security.

The cybersecurity decision-making exercise was conducted during the "Terrorist use of Cyberspace Course" held from March 9-13, 2020 at COE-DAT in Ankara, Turkey. The course sought to familiarize participants with key developments and the emerging threat landscape regarding illegitimate digital opportunity structures and the utilization of cyberspace for crime. This includes the fund-raising, recruitment, communication, propaganda, and training of terrorists. It aims to cultivate understanding of national and international considerations for countering terrorist use of cyber space and to build a stakeholder network around the issue.

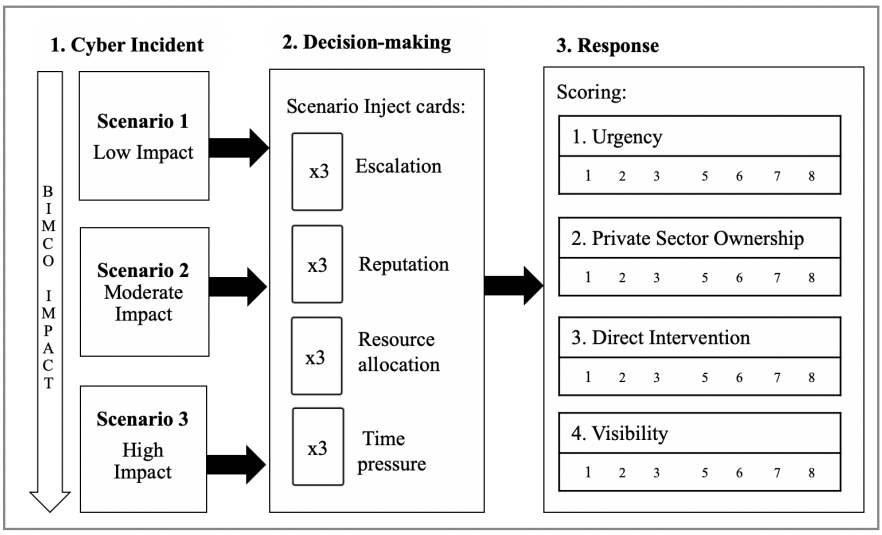
The course is designed for military officers (OF-2/Captain and above) or civilian equivalents (police officers, experts) with minimal formal training in areas such as counter-terrorism and critical infrastructure protection. It was open to select NATO employees, professionals in partner countries and international organizations tasked to respond to cyber incidents. The exercise included participants from 29 countries, all of whom took part to address problems within hybrid nature of emerging maritime cyber threat landscape.

4 Methodology

4.1 Game design

Built on earlier work [14], a cybersecurity decision-making exercise was conducted at a 2020 training course at COE-DAT in Turkey. There were 68 participants in the game. They were divided into four random groups, each with participants from various countries, with mixed work experience and varied cybersecurity expertise. The groups encountered three scenarios that range over cyber incidents in the maritime domain. The scenarios escalate according to BIMCO Impact Levels , outlined in Table 2. For each scenario, participants respond to four scenario inject cards to test decision-making. These are weighted according to the four response attributes to generate score (1-8) which is reported back to them at the end of the game. Results were analysed across groups. The game format is illustrated in Figure 1.

Fig. 1: Game format includes three scenarios with maritime cyber incidents.



4.2 Cyber incident

Participants assume the hypothetical role of "Cyber Incident Lead for the Maritime Response Unit of the National Security Council." As a security

Table 2: BIMCO Impact Levels defined and practical application.

BIMCO Impact Level (Scenario)
1. Limited adverse effect (Low)
Degradation in ship operation to an extent or duration the organisation can perform its primary functions, but effectiveness is clearly reduced. Loss of confidentiality, integrity, or availability (CIA) has a limited adverse effect on company and ship, organisational assets or individuals. Minor- damage to assets, financial loss and harm to individuals.
2. Substantial adverse effect (Moderate)
Significant degradation in ship operation to an extent and duration the organisation can perform its primary functions, but effectiveness is significantly reduced. Loss of CIA has a substantial adverse effect on company, ship, assets or individuals. Significant- damage to organisation assets, financial loss, and harm to individuals (not life-threatening).
3. Severe adverse effect (High)
Severe degradation in or loss of ship operation to an extent and duration the organisation cannot perform at least one primary function. Loss of CIA has a catastrophic adverse effect on company and ship operations, assets, environment or individuals. Major- damage to environment, assets, financial loss and harm to individuals (life-threatening).

Source: BIMCO [2].

official, they advise the head of government and private sector on cyber incident response, with specific regard to Arden Ocean Shipping (AOS), a fictional state-run container shipping company. In this context, participants are presented with three maritime scenarios, summarised in Table 3. However, they are not aware of the escalation. This simulates reality, where decision-makers are often unaware of the severity of an event underway.

Table 3: Summary of the three scenarios that range over cyber incidents in the maritime domain and which escalate according to BIMCO impact levels detailed in Table 2.

Scenario (BIMCO Impact Level)
1. Unicorn of the Sea (Low)
AOS opens an arctic shipping route along Canada as opposed to Russia. The new AOS ice-breakers can access ports previously isolated to trade. This is a sore point for the Canadian Inuit community, as the route crosses waters inhabited by narwhals.The Inuit have spoken out against AOS, claiming ships will disrupt narwhals and may push them to extinction. This issue gains international attention. AOS is reacting to a media storm- many posts originating from Russia. The shipping line opens with *AOS Lunchbox* departing from the Port of Iqaluit. But ship has not departed, as the PCT system that controls cranes that load cargo on the ship has been down for two hours. When they try to to access the system, dockworkers are redirected to the World-Wide Fund for Nature web-page with facts about the narwhal. Dockworkers cannot load the ship ,and must work overtime until this is solved.
2. Parasite (Moderate)
AOS Peru reports Peruvian police found a cocaine in the hull of *AOS Dina* embarking from Peru to Spain when they followed divers in the port, who planted it in a submerged ship compartment. However, when the ship sails the compartment where drugs were hidden is not submerged. The criminals have manipulated the ship OT system which controls ballast, to lower the ship in the water to submerge the compartment, then raise her up- and repeat the process in the port of entry. This is hazardous to crew and cargo, as ballast grounds a ship. The cocaine was confiscated and the divers arrested. Police alerted Spanish authorities for suspicious activity when the ship arrives. However, this group can enter, undetected, into the control systems of at least one AOS liner. Fines associated with transporting illegal substances are large in countries where AOS has a presence, and ships may be arrested in ports of entry.
3. Sitting Duck (High)
AOS Jasmine, a semi-autonomous commercial liner, is stranded in the Persian Gulf. Ground control in the UAE cannot turn on the propeller. The area is known for piracy, but no one has boarded the liner. Communication is being interfered with remotely, stranding the ship across a busy traffic lane. An Algerian oil tanker diverts from course to avoid a collision with the liner, in turn hitting a fishing boat, killing nine. Responding to an SOS in national waters, Iranian military vessels search for survivors and redirect traffic. They also search nearby vessels, as they suspect one may be using a signal jamming device to remotely interfere with liner communication. Ship inspection grows more difficult as a traffic bottlenecks. The CEO of AOS receives an email from an unknown sender which demands the payment of $5 million to a bitcoin account, in exchange for the control of *AOS Jasmine*.

4.3 Decision-making

For each scenario, participants respond to four scenario inject cards, which represent situational changes to the scenario and require decision-making. These were taken from previous research which explored decision-making aspects of a game [14]. Each scenario includes a card which corresponds to the four injects listed and defined in Table 4. Rather than an inject card itself, uncertainty is an overarching factor in the game and there are elements of it in all scenarios. This is because uncertainty is a key component of a crisis [41] and is therefore an assumption in decision-making.

Table 4: The four scenario injects and their operational definition.

Inject	**Definition**
Escalation	Increased severity of incident.
Reputation	Shift in opinion of you or your company, causing loss or damage.
Resource allocation	Available resources to be distributed between two or more things.
Time pressure	Faster response is prompted.

4.4 Response

Four response attributes, based on those developed in previous cybersecurity games [14], are shown in Table 5. Scoring was done by ranking participant response on a scale (1-8), according to their reply to inject cards, whereby each reply has a preassigned weight. Each inject type is paired once with an attribute type, so for example an escalation card may be paired with a situation that teases out visibility, and the response is then added to the final visibility score, whereas each card weighs two points. This was done as an alternative to asking participants to simply rate their perceived response, to avoid confusion around application of terms.

Table 5: Response attributes, expressed as options, and operational definition.

Attribute	**Definition**
Direct intervention	Respond as involved actors, or ask intermediaries to intervene.
Visibility	Respond clearly/openly or ambiguously/behind closed doors.
Private sector ownership	Place responsibility on private or public sector.
Urgency	Choose an immediate or delayed response.

5 Results

5.1 Participants

Prior to the exercise, each of the 68 participants were asked about their work experience and cybersecurity expertise. Figure 2 shows the breakdown of the years spent in public and private sector. Participants exhibited significant experience in the public/military sector (89 per cent had at least five years) and varied private sector experience. It is interesting to note that while all participants reported their public/ military sector experience, over a fourth did not report their private sector experience.

Participants cybersecurity expertise is shown in Figure 3. The group exhibited varied expertise, with the majority of participants rating themselves as either beginner or intermediate (83 per cent). Fewer rated themselves either novice or expert, the two extremes on this spectrum.

Fig. 2: Participants' sector experience by percentage.

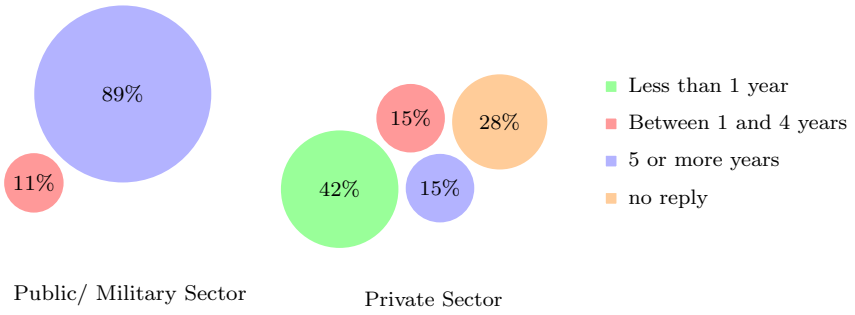
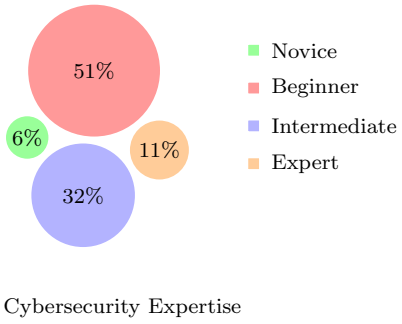


Fig. 3: Participants cybersecurity expertise.

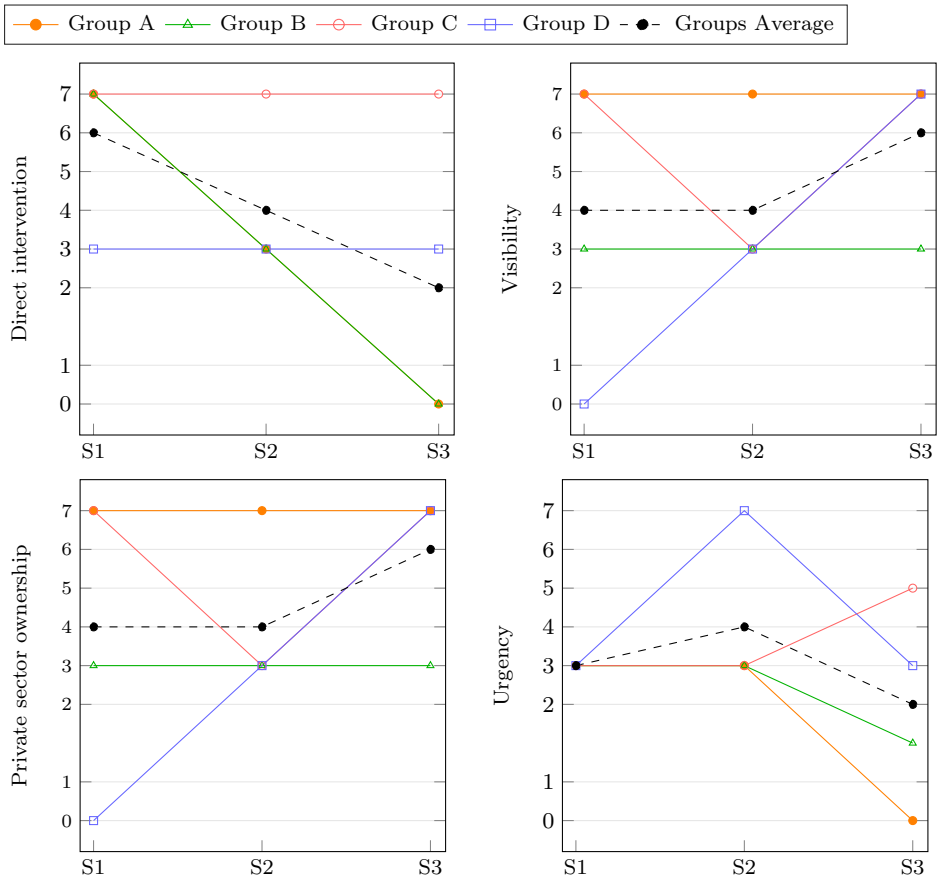


5.2 Effective assessment of risk perception and incident response

In response to the first research question, which asks how risk perception can be effectively assessed, we elected incident classification as a starting point to calibrate risk among decision-makers in a group setting. Incident classification varies greatly, and for this study the BIMCO Impact Levels [2] were selected as a confident measure for the impact of cyber incidents in the maritime sector, as they are currently used and validated in practice. Our game scenarios were constructed to carefully align to these levels, shown in Table 2.

In response to the second question, which asks if work experience and cybersecurity expertise affect cyber incident response, participants rated four response characteristics for each of the three scenarios. Figure 4 shows participant response to the changing impact levels. The trends suggest: The higher the impact of the incident, the response favors of private sector responsibility and visibility, but not urgency or directness.

Fig. 4: Group incident response ranking of scenarios (S1, S2, S3).



6 Discussion

6.1 Understanding and assessing the participant group

In this participant group, there was great diversity in participant response to each response ranking. Figure 4 shows the participant group as a whole did not agree on a uniform response. As shown in Figure 2 and Figure 3, this group had significant public/military sector experience, but varied levels of private sector experience and cybersecurity expertise. Given this information, we may infer that their public/military sector experience may a factor governing their response. This provides a lens through which to interpret the results.

We can confidently say that work experience, more specifically significant public/military sector experience, may affect cyber incident response. Indeed, previous research [48] stresses the importance of *local memory*, or tacit knowledge, in how people make sense of cyber threats or incidents. For this reason, we might expect the results to be framed by a military bias, and a tendency to favor government-led response instead of the private-sector.

Effective assessment of cyber risk perception of experts is done by calibrating risk, according to relevant guidelines, in a group setting. In this sense, we assume the participants, not the researchers, are the experts in the the room. Rather than measuring their results against an external benchmark, the group response as a whole is used to validate response. The value of this measurement increases with the number of participants who take part in the exercise- leading to greater calibration. Thus, the results in this study can be strengthened with further iterations of the game which is a clear direction for future research.

6.2 Comparison of the group results

This section focuses on the trend lines for group average in Figure 4, which suggest: The higher the impact of the incident, the collective response favors private sector responsibility and visibility, but not urgency or directness. Accounting for significant work experience in the military/public sector, we may interpret the results of this study to understand tendencies of the participant group and infer about cyber incident response behaviors of NATO military officers and equivalent civilians. These offer insights on tendencies which characterise the NATO security culture, from which emerges a collective risk perception.

First, group urgency of response decreases along with the impact of a cyber incident. This may reflect the idea that while small-scale cyber-attacks may be the work of criminals, larger-scale attacks are more likely the work of organised or skilled actors (e.g. states) with increased resources to support a complex attack and a long-term outlook. In this sense, “Law enforcement and military authorities seeking to check malicious cyber activity face another fundamental challenge: the ‘attribution problem’ of identifying the author of a cyber attack

or cyber exploitation" [9]. While there may be pressure to name an adversary, the consequences of naming the wrong one early on often outweigh the cost of delaying response while information is gathered and verified. Indeed, the main hurdle is verification, which is difficult in the cyber realm due to attribution [9].

Second, as incident impact increased, the group favored a response led by the private sector, as opposed to the government, although the response did include a combination of both. This is interesting finding, as we estimated there would be a tendency to favor government-led response because in many countries military is closely aligned to state. Further, the 2019 Global Cyber Risk Perception Survey reports a "strong appetite for government leadership and support" to help combat cyber threats [25]. However, the opposite is observed: as impact increased, group response favored the private sector.

One explanation is that as a cyber incident escalates, the government becomes reluctant to claim mandates to oversee network security. Yet, it is often the case that the private sector is not inclined to accept responsibility or liability for national cybersecurity. This tendency is noted in previous work [4] concerning the challenges of public-private-partnerships. Another factor at play is that "the private sector has their hands deep in cyberspace in a way very difficult for the government to match" [12]. Wide expansion of IT products and services- a process now catalysed by COVID-19- makes it difficult for the government to keep up with the private sector, thus they rely on it. Consider that nearly 90 per cent of US critical infrastructure is in private hands [49]. It is plausible this participant group, who comprise largely of military officers, are aware of this fact and thus rely on the private sector.

Third, group visibility of response increased along with incident impact. This may have to do with a the fact that, while smaller incidents are easier to keep hidden or covert, large-scale cyber attacks are difficult to hide. Therefore, visibility reflects a greater need for assurance to those affected by and aware of the incident, for instance the public or the international community.

Finally, as incident impact increased, group response was less direct. This may be because as the impact of a cyber incident increases, so does its scale and complexity– to a point that a collective and multi-faceted response is required, especially in the context of NATO and- further- during a pandemic. This is evidenced in the previous example of "Cozy Bear" targeting COVID-19 vaccine researchers [30], where NATO was the first body to indirectly articulate information collected by various allies, including Canadian, UK, and US government institutions.

6.3 Implications for practice

This study outlines key implications of digital acceleration on maritime cybersecurity and investigates NATO collective cyber risk perception. It offers insights into cyber risk- in all its complexity- at a time when it has never been more relevant or misunderstood. COVID-19 has led to greater reliance on technology and new digital opportunity structures that increase

cyber risk. Our cybersecurity decision-making exercise provides a way for decision-makers to grow familiar with acting amidst uncertainty, an over-arching factor in cyber incident response. Further, "the simulation environment provides a context in which can implement various strategies in any number of repetitions without fear of real consequences" [18].

This study also offers unique insights into risk perception, a major aspect in maritime cyber risk management that, while complex, is key to effective decision-making and cyber incident response [51]. Our cyber exercise demonstrates that cyber risk perception can be not only measured, but improved significantly through iterative learning.

There is a great need for cybersecurity training tools within the maritime community that reinforce proportionate response to cyber incidents. NATO has made efforts to strengthen cybersecurity, evidenced in the over 200 training courses conducted at the COE-DAT center. Despite these efforts, current training has not achieved shared situational awareness on cyber threats across their partners [21]. NATO can benefit from the findings of this study by incorporating cybersecurity decision-making exercise environments in their training, to challenge risk perceptions and strengthen a shared security culture. Further, this exercise is a tool for actors across the maritime community, including industry, government, and international organisations.

7 Conclusion

Using our cybersecurity decision-making exercise, we focus on understanding how a group from a NATO Centre of Excellency perceives cyber risk and responds to cyber incidents in the maritime domain. In general, two main findings contribute to maritime cyber risk perception and response:

- Effective assessment of collective cyber risk perception can be done by calibrating risk, according to relevant sector guidelines, in a group setting.
- As incident impact rises, groups with strong public/military sector experience and mixed cybersecurity expertise respond in favor of private sector responsibility and visibility, but not in favor urgency or directness.

As maritime organizations modernise and embrace accelerated digitisation due to COVID-19, they must take steps to prevent and defend against cyber threats. This exercise is a tool to prepare robust cyberspace operations. Effective risk perception and response are key to cyber risk management. This exercise, trialled successfully in small setting, offers insights into capacity building and echoes the need for joint response.

In the words of Andrea Carcano, co-founder of Nozomi Networks, "Technology is available to give asset owners the insight they need into their devices, connections, and communications. With the right technology and a focus on best practices, maritime organizations can increase operational resiliency." [10] They can come out of this ongoing pandemic more connected, coordinated, and resilient- ready to navigate new digital waves.

References

1. Barnes, S.J.: Information management research and practice in the post-covid-19 world. International Journal of Information Management **55**, 102175 (2020)
2. BIMCO, CLIA, ICS, Intercargo, Intermanager, Intertanko, IUMI, OCIMF and World Shipping Council: The guidelines on cyber security onboard ships- version 3 (2018)
3. Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., Díaz-Castaño, N.: Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies pp. 1–13 (2020)
4. Carr, M.: Public–private partnerships in national cyber-security strategies. International Affairs **92**(1), 43–62 (2016)
5. Coburn, A.: The great acceleration and cyber risk (2020). Cyber Risk Conference 2020: The Cyber Ecosystem
6. Collier, B., Horgan, S., Jones, R., Shepherd, L.: The implications of the covid-19 pandemic for cybercrime policing in scotland: A rapid review of the evidence and future considerations. Scottish Institute for Policing Research (2020)
7. 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/
8. De Smidt, G., Botzen, W.: Perceptions of corporate cyber risks and insurance decision-making. The Geneva Papers on Risk and Insurance-Issues and Practice **43**(2), 239–274 (2018)
9. Goldsmith, J.: How cyber changes the laws of war. European Journal of International Law **24**(1), 129–138 (2013)
10. Grasso Macola, I.: US Tugboat cyber-attack: the experts respond (2020). URL https://www.ship-technology.com/features/cyber-attacks-in-the-maritime-sector-the-experts-respond/
11. Greenberg, A.: The Untold Story of NotPetya, the Most Devastating Cyberattack in History (2018). URL https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
12. Healey, J.: Who's in control: Balance in cyber's public-private sector partnerships. Geo. J. Int'l Aff. **18**, 120 (2017)
13. Hubbard, D.W.: The failure of risk management: Why it's broken and how to fix it. John Wiley & Sons (2020)
14. Hussain, A., Kuhn, K., Shaikh, S.A.: Games for cybersecurity decision-making. In: HCI-Games: 2nd International Conference on HCI in Games, pp. In–press. Springer (2020)
15. Hussain, A., Shaikh, S., Chung, A., Dawda, S., Carr, M.: An Evidence Quality Assessment Model for Cybersecurity Policymaking, vol. (542), pp. (23–38). Springer, Cham (2018). DOI https://doi.org/10.1007/978-3-030-04537-1_2
16. International Chamber of Shipping: Shipping and world trade (2020). URL https://www.ics-shipping.org/shipping-facts/shipping-and-world-trade
17. International Transport Forum: Itf transport outlook 2019 (2019). DOI https://doi.org/https://doi.org/10.1787/transp_outlook-en-2019-en. URL https://www.oecd-ilibrary.org/content/publication/transp_outlook-en-2019-en
18. Jalali, M.S., Siegel, M., Madnick, S.: Decision-making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment. The Journal of Strategic Information Systems **28**(1), 66–82 (2019). DOI https://doi.org/10.1016/j.jsis.2018.09.003. URL http://www.sciencedirect.com/science/article/pii/S0963868717304353
19. Konrad, J.: IMO Cyber-attack Has Serious Implications (2020). URL https://gcaptain.com/imo-cyberattack-has-serious-implications/
20. Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X.: Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. arXiv preprint arXiv:2006.11929 (2020)
21. Lété, B., Pernik, P.: EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions. German Marshall Fund of the United States (2017)

22. Maliszewska, M., Mattoo, A., Van Der Mensbrugghe, D.: The potential impact of covid-19 on gdp and trade: A preliminary assessment (2020)
23. Malynn, K.: Damage limitation following a cyber-security breach (2020). Maritime Cyber Risk Management, Europe, Virtual Conference
24. Markit, I.: Safety at Sea and BIMCO cyber security white paper (2020). URL https://cdn.ihsmarkit.com/www/prot/pdf/1020/Safety-at-Sea-and-BIMCO-Cyber-Security-White-Paper-2020.pdf
25. Marsh LLC and Microsoft: 2019 global cyber risk perception survey (2019). URL https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf
26. Miró-Llinares, F., Moneva, A.: What about cyberspace (and cybercrime alongside it?) A reply to Farrell and Birks "Did cybercrime cause the crime drop?". Crime Science **8**(1), 12 (2019)
27. National Cyber Security Centre: Uk and allies expose russian attacks on coronavirus vaccine development (2020). URL https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development
28. Network, A.J.M.: Israel cyberattack caused 'total disarray' at iran port: Report. URL https://www.aljazeera.com/news/2020/5/19/israel-cyberattack-caused-total-disarray-at-iran-port-report
29. North Atlantic Treaty Organization: Active engagement, modern defence: Strategic concept for the defence and security of the members of the north atlantic treaty organization (2010)
30. North Atlantic Treaty Organization: Statement by the north atlantic council concerning malicious cyber activities (2020). URL https://www.nato.int/cps/en/natohq/official_texts_176136.htm
31. Organisation, I.M.: The interruption of service was caused by a cyber attack against our IT systems. IMO is working with @UN IT and security experts to restore systems as soon as possible, identify the source of the attack, and further enhance security systems to prevent recurrence. (2020). URL https://twitter.com/IMOHQ/status/1311601524209049601/photo/1. Tweet: 1311601524209049601
32. Papadopoulos, T., Baltas, K.N., Balta, M.E.: The use of digital technologies by small and medium enterprises during covid-19: Implications for theory and practice. International Journal of Information Management (2020)
33. Reynolds, Z.: Toll Logistics hit by second cyber attack (2020). URL https://safetyatsea.net/news/2020/cyber-crimes-land-second-hit-on-toll-logistics/
34. for Risk Studies, C.C.: Shen attack: Cyber risk in asia pacific ports (2019). URL https://www.msig-asia.com/sites/msig_asia/files/downloads/CyRiM_ShenAttack_FinalReport.pdf
35. Cambridge Centre for Risk Studies, U.o.C.: Cambridge centre for risk studies, 2019; global risk index 2020 executive summary (2019)
36. Rogers, G.O.: Residential proximity, perceived and acceptable risk. In: Low-Probability High-Consequence Risk Analysis, pp. 507–520. Springer (1984)
37. Schofield, C.: What's at stake in the south china sea? geographical and geopolitical considerations. In: Beyond Territorial Disputes in the South China Sea. Edward Elgar Publishing (2013)
38. Shapira, Z.: Risk taking: A managerial perspective. Russell Sage Foundation (1995)
39. Shen, C., Baker, J.: CMA CGM confirms ransomware attack (2020). URL https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack
40. Smith, J., Doody, K., Veitch, B.: Being prepared for emergencies: a virtual environment experiment on the retention and maintenance of egress skills. WMU Journal of Maritime Affairs **18**(3), 425–449 (2019)
41. Stern, E.: Designing crisis management training and exercises for strategic leaders: A Swedish and United States Collaborative project. National Defense College (2014)
42. Svilicic, B., Kamahara, J., Celic, J., Bolmsten, J.: Assessing ship cyber risks: a framework and case study of ecdis security. WMU Journal of Maritime Affairs **18**(3), 509–520 (2019)

43. Tam, K.: What are the cyber threats to shipping? (2020). URL https://www.plymouth.ac.uk/news/pr-opinion/keeping-the-fleet-sailing-during-covid-19
44. Tam, K., Jones, K.: Cyber-risk assessment for autonomous ships. In: 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp. 1–8. IEEE (2018)
45. Thunstrom, L., Newbold, S., Finnoff, D., Ashworth, M., Shogren, J.F.: The benefits and costs of flattening the curve for covid-19. SSRN 3561934 (2020)
46. Twining, G.: IMO hit by 'sophisticated' cyber attack (2020). URL https://safetyatsea.net/news/2020/the-imo-hit-by-sophisticated-cyber-attack/
47. Twining, G.: MSC confirm malware attack (2020). URL https://safetyatsea.net/news/2020/msc-confirm-malware-attack/
48. Walker, G., Simmons, P., Wynne, B., Irwin, A.: Public perception of risks associated with major accident hazards. HSE Contract Research Report (1998)
49. Weinstein, D.: America's cyber blind spot. Geo. J. Int'l Aff. (2019)
50. Wiese Bockmann, M.: Seized uk tanker likely 'spoofed' by iran (2019). URL https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran
51. Williams, M.J.: NATO, security and risk management: from Kosovo to Khandahar. Routledge (2008)
52. Worldwide, A.: Global ecommerce retail sales up 209 percent in april (2020)
53. Young, R., Malynn, K.: Marine: Silent cyber at sea (2020). URL https://https://www.beazley.com/beazley_academy/marine_cyber_silent_at_sea.html