WMU Journal of Maritime Affairs (2021) 20:193–214
https://doi.org/10.1007/s13437-021-00235-1

ARTICLE

COVID-19 digitization in maritime: understanding cyber risks

Kristen Kuhn[1] · **Salih Bicakci**[2] · **Siraj Ahmed Shaikh**[1,3]

Received: 2 December 2020 / Accepted: 8 April 2021 / Published online: 22 June 2021

Abstract

Digitization is reshaping the maritime industry which is under increasing pressure to transform. Technology is more common as it offers improvements and carves out early adapters as more competitive. COVID-19 hastens digitization and creates new digital opportunity structures which increase cyber risks. Cyber attacks, which can cripple critical systems and services at significant cost, motivate stakeholders to engage with these risks. This paper reviews current events and introduces an exercise where participants at a NATO Centre of Excellency were shown scenarios involving maritime cyber incidents and evaluated on cyber risk perception. Our findings lend insight on how to assess group cyber risk perception—and how this impacts response. They highlight the need to plan for cyberspace operations and ground cyber risks as a intricate governing factor in maritime.

Keywords Cyber risk perception · Decision-making · Maritime security

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" International Maritime Organisation (2020). This attack had serious implications, coming at a time when the IMO was under intense scrutiny, working to bring attention to the global

✉ Kristen Kuhn
kristen.kuhn@coventry.ac.uk

Salih Bicakci
asbicakci@khas.edu.tr

[1] Systems Security Group, Institute for Future Transport and Cities, Coventry University, Coventry, UK

[2] Department of International Relations, Kadir Has University, Istanbul, Turkey

[3] Security, Risks Management and Conflict, Research Group, Universidad Nebrija, Madrid, Spain

crew crisis,and—-ironically—asking its members to enforce IMO 2021, a resolution requiring ship owners to invest in cybersecurity (Konrad 2020).

The IMO was the second major shipping organization to be hit by a cyber attack that week, and the fifth high-profile attack in 2020 (Twining 2020a). It came 3 days after shipping giant CMA CGM reported a ransomware attack (Shen and Baker 2020). The logistics company Toll Group was also hit by two distinct ransomware attacks, in January and in May 2020 (Reynolds 2020). Mediterranean Shipping Company (MSC) suffered a malware attack at its Geneva headquarters in April (Twining 2020b). Lallie et al. (2020) suggests the surge in attacks this year is a result of the mass disruption worldwide caused by the pandemic, while Pandey et al. (2020) points to increased reliance on digital services due to COVID-19.

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 and, in particular, why cyber risk perception is a key factor but also a difficult one to grasp. This is done using a game-based method, which includes a structured, scenario-driven exercise through which we asses participant response to three hypothetical cyber incidents. We draw insights on cyberawareness and implications for practice from a pre-exercise survey, scored exercise responses and post-exercise discussion.

In June 2020, The North Atlantic Treaty Organization (NATO) issued a statement (North Atlantic Treaty Organization 2020) condemning cyber attacks inflicted amidst the ongoing global health pandemic. NATO, an intergovernmental military alliance that extends to the maritime domain, must address COVID-19 and its cybersecurity significance. Yet, some argue its members lack a shared situational awareness on cyber threats (Lété and Pernik 2017) which may 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 developed a cybersecurity decision-making exercise which was conducted at a March 2020 NATO training course at The Centre of Excellence Defence against Terrorism (COE-DAT). Using scenarios that range over maritime cyber incidents, we examine the cyber risk perception 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 characterize NATO security culture. We then discuss implications for practice and interpret findings in the context of COVID-19. 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 organizations, 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" (Lété and Pernik 2017). 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. The findings presented in this paper were processed from a pre-exercise survey, scored exercises responses, and a post-exercise discussion.

The rest of this paper is organized as follows: Section 2 investigates COVID-19 and its implications for maritime cybersecurity, and explores maritime cyber risk. Section 3 introduces NATO as a case study and presents The Center of Excellence Defence against Terrorism (COE-DAT). Section 4 details our methodology which includes the development of a structured, scenario-driven exercise through which we explore cyber risk perception. Section 5 presents results, including our findings on participants background, risk perception and incident response. Section 6 discusses these results to understand and assess participants and draws implications for practice. Conclusions, including main findings and their relevance to COVID-19, are found in Section 7.

2 Background

2.1 COVID-19 and its implications for maritime cybersecurity

The global COVID-19 lockdown of 2020 disrupted the world economy. Four billion people (51% of the world's population) were locked down by government mandate in the first half of the year (Coburn 2020). Citizens were unable to work, visit shops, travel or socialize. This lockdown led to a 4% reduction in global GDP (Maliszewska et al. 2020) and resulted in over $5 trillion of output lost in 6 months (Thunstrom et al. 2020). 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 (Coburn 2020).

Although this paper is focused on COVID-19, this has only accelerated an existing technological transformation of our society and economy (Shaikh 2017). Technology was already more common because it improves physical safety, efficiency, communication and training. Consider that most physical processes in the maritime sector are now performed with at least semi-automated mechanical systems and machinery under the control of sophisticated software systems (Kuhn et al. 2020).

Like cyberspace, technology evolves along with our perception of it. Xiang (2018) notes a shift from Digitization (1997–2006) to the Age of Acceleration (2007–2016). In particular, he recognizes a shifting view of IT from a primarily marketing-driven tool to a knowledge creation tool due to new considerations like big data which can facilitate, for instance, fuel consumption of ships. Kamphake (2020) also recognizes this shift while exploring digitization in controlling, where he observes that both managing and harnessing data for business is moving towards the use of predictive analytics. Corporate management can use modern statistical algorithms to find patterns, trends, and structures more accurately. This accuracy will improve as efficiency pressure increases and companies respond to market changes amidst rapidly globalizing competition.

Technology carves out early adapters as more competitive than ever before. This holds true for those who adapt to new challenges associated with the COVID-19 pandemic. New technologies have risen in the maritime industry in response to COVID-19 including, for instance, track and trace, the rise of e-documents and increased supply chain resilience through block-chain (Yam 2021).

The looming pandemic has many researchers investigating just how much digital change COVID-19 has caused organizations (Papadopoulos et al. 2020). Early results show that digitization has increased significantly (Coburn 2020) during the global lockdown and that, as a result, cyber crime is on the rise (Miró-Llinares and Moneva 2019). This speaks to a larger trend: As organizations rely more on technology, their level of cyber risk increases. This trend acknowledges increased digitization as a key factor to increased cyber risks, but not the only one. Apart from lacking cyber awareness, people's vulnerabilities may have also increased because they used existing technology more (in addition to there being more of it). More people are now unemployed, spend more time at home and use the Internet for work and to socialize (Pranggono and Arabo 2020). These situations can overwhelm many, causing anxiety that can alter risk behavior (e.g., excessive COVID-19-related Internet use as safety-seeking behavior) and increase their chances of falling victim to an attack (Jungmann and Witthöft 2020). Rapid societal transformations experienced during the outbreak, which have increased the frequency and variety of online activity, have created new opportunity structures (Lallie et al. 2020)—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% in April 2020 alone (ACI Worldwide 2020). During lockdown, online shopping reached mammoth proportions, as new and existing online consumers seek to obtain products via available means (Barnes 2020).

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 (Barnes 2020). Pandey et al. (2020) reported in June 2020 that internet services had risen in usage from 40 to 100%, compared to pre-lockdown levels and the use of

video-conferencing services increased tenfold. According to Ido Ben-Moshe, Vice President of Business Development at Naval Dome, remote working and an increase in remotely controlled, autonomous technologies will continue to accelerate during and after COVID-19 (Twining 2020a).

Navigating the new world in terms of online trade and remote working is not without its challenges. While digitization fosters business opportunities, it adds complexity to security protection and makes systems more valuable. Limited security awareness of employees in these new conditions have compounded these challenges (Coburn 2020). According to Ben-Moshe, "companies [will] face new cyber security challenges if they fail to implement adequate protective measures" (Twining 2020a). 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" (Grasso 2020). While Akthar is correct, most cyber incidents are outcomes of human error—or they are exploited by accident, it is worth mention that cyber crime 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 (Miró-Llinares and Moneva 2019). Early research (Lallie et al. 2020) 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 an increase in all areas of cyber crime (Tam 2020). That is, increased digitization brings increased cyber risk. Buil-Gil et al. (2021) 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. (2020) observe increased denial of service attacks and Coburn (2020) points to increases in ransomware attacks and in the activity of state-sponsored groups stemming from geopolitical tensions.

Rising cyber crime 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 organizations experienced cyber attacks—a 9% increase from the previous year (Markit 2020). Akin to Buil-Gil et al. (2021), this study also identified fraud as the main cyber incident in the maritime sector, including phishing (68% of attacks) and spear phishing (41%). Malware was the third most common incident (33%).

2.1.3 Implications for maritime cybersecurity

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 (Coburn 2020). Thus, COVID-19 has driven a major increase in cyber risk.

Indeed, the pandemic has especially wide implications for the maritime sector, where global shipping 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 partners and shipped goods. JIT saves a lot of money spent holding things in stock, but creates vulnerabilities if shipments are delayed or lost (Tam 2020). Operational shutdowns, a consequence of cyber attacks, can cause costly disruptions that ripple through vulnerable systems and networks (Cyberhedge 2020). Currently, these supply chains are badly stretched due to COVID-19, adding immense pressure on organizations to quickly restore any loss of control of IT systems and resume normal operations. This was the case for Mediterranean Shipping Company (MSC), who fell victim to a cyber attack in April 2020 (Twining 2020b), when 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, digitization was a growing factor in shipping before COVID-19, making cybersecurity increasingly relevant. One only needs recall the 2017 Not-Peta ransomware attack on Maersk, which disrupted their operations for 2 weeks, resulted in a 20% 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 (Cyberhedge 2020). This attack has driven the importance of cybersecurity home for many, and has since become an almost legendary cyber attack in maritime. Organizations 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 2 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% through 2050, and that maritime trade volumes will almost triple (International Transport Forum 2019). 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.

2.2 Understanding maritime cyber risk

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 (Grasso 2020). Allianz Global Corporate and Specialty SE (2019) found a worst-case scenario involving the collision of two large vessels in an environmentally-sensitive location could result in significant loss of life, untold

Table 1 Eight recent cyber attacks in the maritime industry, including the date, target, affected systems (IT, OT), impact, and a brief attack description

Date	Target	Systems	Impact	Description
10/20	IMO	IT	-Network outage	Malware attack that disabled their website and intranet, forcing the UN organization to shut down key systems to prevent further damage (Konrad 2020).
09/20	CMA CGM	IT	-Network outage -Data infiltration	Ransomware attack on its Chinese offices, forcing the container line to shut down network and online services to prevent further damage (Shen and Baker 2020).
09/20	US tug boat	IT	-Email spoofing	Phishing attack involving a malware email which spoofed the vessel operator, who sent it to the vessel via an email attachment (Grasso 2020).
01/20	Toll Group	IT	-Data theft -Network outage	Ransomware attack using 'Netwalker' software that hit land and sea operations. The attackers shut down systems, caused delays and disruptions, attributed to Russian hackers (Reynolds 2020).
04/20	MSC	IT	-Network outage	Malware attack that affected systems at the shipping line's Geneva headquarters, resulting in disruption but minimal damage (Twining 2020b).
06/20	Toll Group	IT	-Data theft -Network outage	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 (Reynolds 2020).
06/20	Shahid Rajaee Port	IT, OT	-Data infiltration -Damaged operating systems	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 (Al Jazeera Media Network 2021).
07/19	*Stena Impero*	OT	-GPS spoofing -GPS outage -Navigation disruption	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 (Wiese Bockmann 2019).

environmental damage, and financial losses up to $4 billion "when the cost of disruption, salvage, wreck removal, and environmental claims are considered." That is the potential extent of damage if the navigational computer systems on one ship are hacked. It is difficult, then, to envision the damage that would occur if a hacker entered into the same systems which control an entire global fleet of vessels (Konrad 2020), by which a *fleet* consists of numerous ships connected to and operating under a unified control unit. Another 2019 study by The Cambridge Centre for Risk Studies considers the damage associated with a cyber attack where a computer virus infects 15 major ports across Asia Pacific and estimates economic loss upwards of $110 billion (For Risk Studies 2019).

Maritime cybersecurity incidents can take many forms. Areas of marine cyber risk include physical damage, loss of availability and extortion (Malynn 2020). 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/safety, delay or disruption, and various types of business risks (Centre for Risk Studies 2019) (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 (Hubbard 2020). Understanding maritime cyber risk is a challenge as it is complex, evolving, and asymmetrical (De Smidt and Botzen 2018); larger attack surfaces and greater uncertainty makes it hard to assess risk and formulate response. Accelerated digitization, a result of COVID-19, is associated with increased cyber risk and that means less time for organizations to prepare response. While cyber incidents are inevitable, and risk cannot be eliminated, it can be managed.

2.2.1 Cyber risk perception

Risk perception is relevant to leaders because it influences their decision-making. Misjudgements, often due to erroneous risk perception, can lead to disproportionate response such as mistakes in resource allocation or incident escalation. In other words, gaps in perception of risk indicate gaps in capabilities to act (Williams 2008).

It is acknowledged that, among other factors, perception rests on a foundation of experience (Rogers 1984). Those who have not already responded to a previous 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, be it negative or positive. Indeed, these two aspects—positive and negative—make risky choice play a central role in decision-making under uncertainty (Shapira 1995).

One way to learn about perceived risk is examine response to real or hypothetical events. For instance, a 2019 study (Smith et al. 2019) proposes a virtual environment to observe egress skills on offshore petroleum platforms. Four such training exercises, with simulation environments applicable to the transport sector, are listed in

Table 2. The exercise-based approach in this study is demonstrated (Jalali et al. 2019) to improve incident response by iterative learning.

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 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" (Williams 2008).

This study includes 68 participants with varied levels of cyber expertise. It is a unique sample 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, calibration indicates effective risk assessment and streamlined risk perception.

Table 2 Four training exercises with simulation environments applicable to the transport sector, including exercise, sector, target audience and objective

Exercise	Sector	Target audience	Objective
AVERT Simulator	-Maritime	-Crews/personnel, offshore petroleum platforms	Proposed a virtual environment to observe egress skills on offshore petroleum platforms (Smith et al. 2019).
Cybersecurity Decision-making Game	-Automotive *Can adapt to different sectors	-Decision-makers -Executives -Policy makers	Proposed a simulation game to assess cybersecurity decision-making skills (Hussain et al. 2020).
CyberMAR	-Maritime *Can adapt to different transport subsectors	-Decision-makers -Public authorities -International organizations -Academia	Developed a simulation environment that seeks to unlock the value of using cyber range in the maritime logistics value chain (Canepa et al. 2020; Ouzounoglou 2021.)
MIT Cybersecurity Simulation Game	-Different industry sectors	-Decision-makers -Executives -Managers	Developed a simulation game to study cybersecurity complexities: delays in capability development and incident uncertainty (Jalali et al. 2019).

3 Case study: NATO collective cyber risk perception

In June 2020, NATO issued a statement (North Atlantic Treaty Organization 2020) to condemn cyber attacks inflicted during 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 (National cyber security centre 2020). 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 recognize an attack, NATO served as a collective body to communicate information—over a month before its members did so independently. This is an active demonstration of NATO's three core tasks, as defined in the 2010 Strategic Concept (North Atlantic Treaty Organization 2010): collective defense, crisis management and cooperative security. It also outlines the big achievement of NATO: collective response.

It's not always that easy. Complexity is 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 with NATO, states can cultivate a group risk culture and agree to support group response. However, this can be problematic when not all members 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 members (Lété and Pernik 2017). 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 members. 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

The 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 cyberspace 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 and professionals in member states, employed at international organizations that respond to cyber incidents. It should be mentioned that a small number of participants were from NATO partner states (North Atlantic Treaty Organisation 2020) that are non-member states (e.g., Pakistan, considered a "Partner across the globe" had 1 participant). The exercise included a total of 68 participants from 29 countries, shown in Fig. 1, all of whom took part to address problems within the emerging maritime cyber threat landscape.

4 Methodology

4.1 Exercise design

Built on earlier work (Hussain et al. 2020), 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

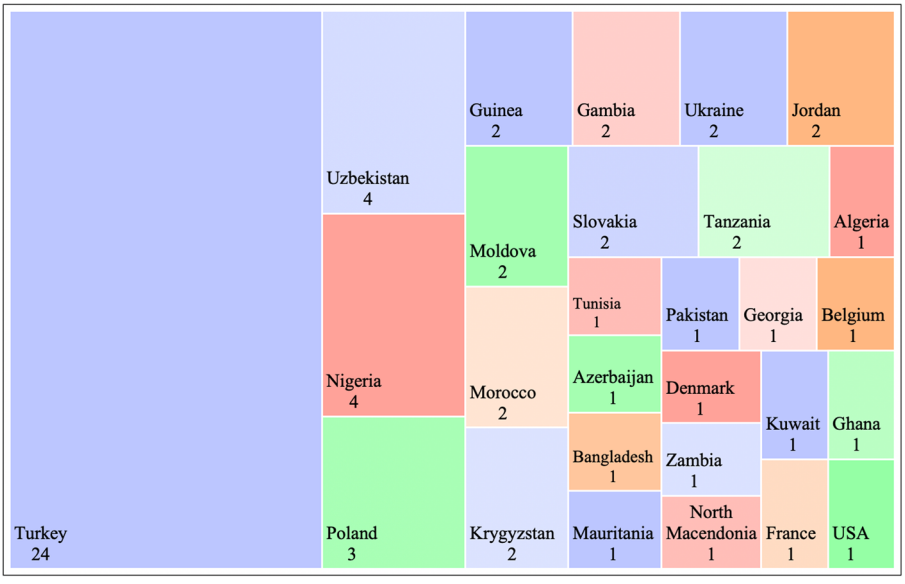


Fig. 1 The exercise included a total of 68 participants from 29 countries

Table 3 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 organization 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, 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 organization 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 assets, financial loss, and harm to individuals.
3. Severe adverse effect (High) Severe degradation in ship operation to an extent and duration the organization 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 or loss of life.

Source: BIMCO (2018)

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 3. 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 a score (1–8) which is reported back to them

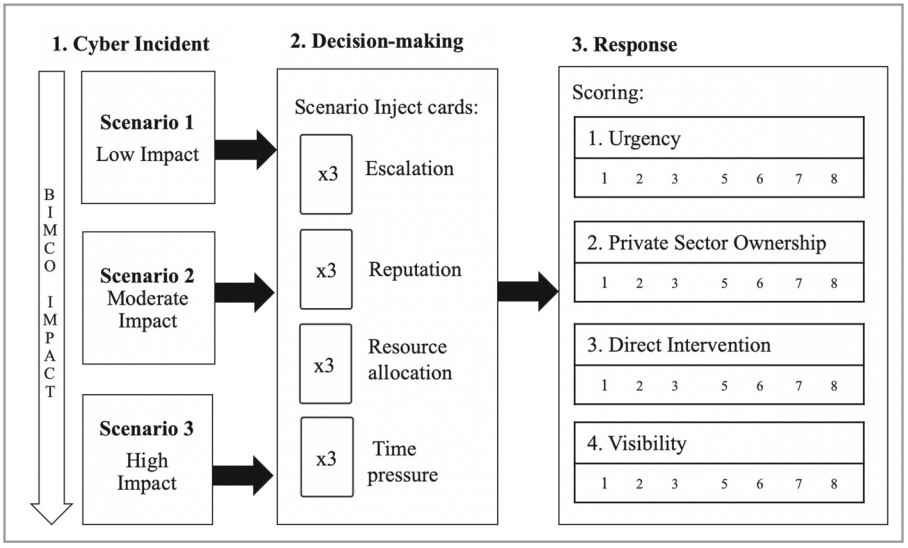


Fig. 2 Game format includes three scenarios with maritime cyber incidents

at the end of the game. Results were analyzed across groups. The game format is illustrated in Fig. 2.

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 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, summarized in Table 4. However, they are not aware of the escalation. This

Table 4 Summary of the three scenarios that include maritime cyber incidents, which escalate according to BIMCO impact levels detailed in Table 3

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 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*.

Table 5 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.

simulates reality, where decision-makers are often unaware of the severity of an event underway.

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 (Hussain et al. 2020). Each scenario includes a card which corresponds to the four injects listed and defined in Table 5. 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 (Stern 2014) and is therefore an assumption in decision-making.

4.4 Response

Four response attributes, based on those developed in previous cybersecurity games (Hussain et al. 2020), are shown in Table 6. 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

Table 6 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.

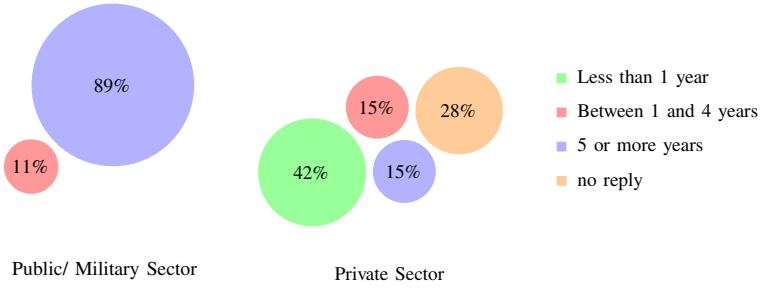


Fig. 3 Participants' sector experience by percentage

to simply rate their perceived response, to avoid confusion around application of terms.

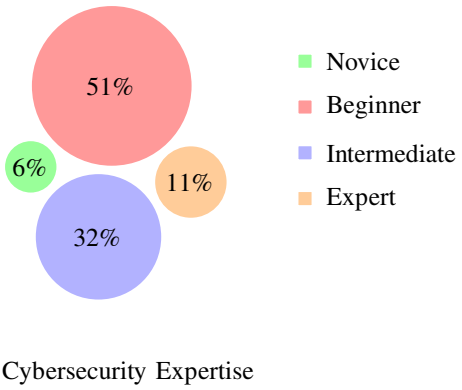
5 Results

5.1 Participants

Prior to the exercise, each of the 68 participants were asked about their work experience and cybersecurity expertise. Figure 3 shows the breakdown of the years spent in public and private sector. Participants exhibited significant experience in the public/military sector (89% had at least 5 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 Fig. 4. The group exhibited varied expertise, with the majority of participants rating themselves as either beginner or intermediate (83%). Fewer rated themselves either novice or expert, the two extremes on this spectrum.

Fig. 4 Participants cybersecurity expertise



5.2 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 (BIMCO 2018) 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 3.

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 5 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.

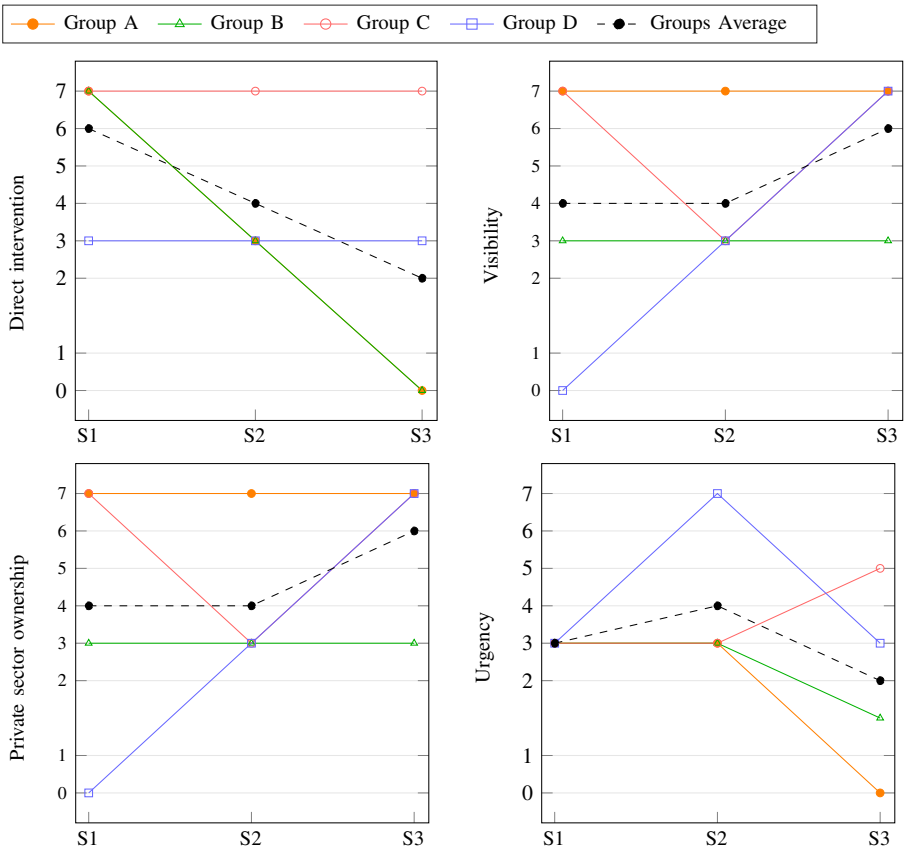


Fig. 5 Group incident response ranking of scenarios (S1, S2, S3)

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 5 shows the participant group as a whole did not agree on a uniform response. As shown in Figs. 3 and 4, 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 (Walker et al. 1998) 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 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 Fig. 5, 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 characterize 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 organized 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" (Goldsmith 2013). 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 (Goldsmith 2013).

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 (Marsh LLC and Microsoft 2019). 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 (Carr 2016) 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" (Healey 2017). Wide expansion of IT products and services—a process now catalyzed 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% of US critical infrastructure is in private hands (Weinstein 2019). 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 (North Atlantic Treaty Organization 2020), 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 COVID-19 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 overarching 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" (Jalali et al. 2019).

This study also offers unique insights into risk perception, a grounding aspect in maritime cyber risk assessment that, while complex, is key to effective decision-making and cyber incident response (Williams 2008). 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 members (Lété and Pernik 2017). 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 organizations.

7 Conclusion

The year of 2020 will be remembered as uniquely disruptive — but not just for a global health crisis. Online life has been digitally transformed, as exponential change accelerated at home and work via cyberspace (Lohrmann 2020). Even before COVID-19, the maritime industry was under increasing pressure to transform. The global lockdown has accelerated digitization significantly (Coburn 2020) and underscored the importance of technology in this process (Yam 2021). As maritime organizations embrace accelerated digitization, they must take steps to prevent and defend against cyber threats. This includes being able to effectively perceive increased cyber risks associated with new and increased use of technology—and it implications.

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.

This exercise is a tool to prepare robust cyberspace operations. Effective risk perception and response are key to cyber risk assessment. 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." Grasso (2020). They can come out of the COVID-19 pandemic more connected, coordinated, and resilient—ready to navigate new digital waves.

References

Allianz Global Corporate and Specialty SE (2019) Safety and shipping review 2019. https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/press/document/AGCS_shipping_review_2019.pdf

Al Jazeera Media Network (2021) Israel cyberattack caused total disarray at Iran port: Report. https://www.aljazeera.com/news/2020/5/19/israel-cyberattack-caused-total-disarray-at-iran-port-report

Barnes SJ (2020) Information management research and practice in the post-covid-19 world. Int J Inf Manag 102175:55

BIMCO (2018) The Guidelines on Cyber Security Onboard Ships- Version 3. BIMCO, CLIA, ICS, Intercargo, Intermanager, Intertanko, IUMI, OCIMF and World Shipping Council. https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cybersecurity-onboard-ships-min.pdf

Buil-Gil D, Miró-Llinares F, Moneva A, Kemp S, Díaz-Castaño N (2021) Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies 23(sup1):S47–S59

Canepa M, Ballini F, Dalaklis D, Vakili S, Hernandez LMC (2020) Effectiveness of Cybersecurity Training and Awareness Raising within the Maritime Logistics Domain

Carr M (2016) Public–private partnerships in national cyber-security strategies. Int Aff 92(1):43–62

Coburn A (2020) The Great Acceleration and Cyber Risk. https://www.jbs.cam.ac.uk/faculty-research/centres/risk/news-events/events/2020-events/the-cyber-ecosystem-2020/

Collier B, Horgan S, Jones R, Shepherd L (2020) 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

Cyberhedge (2020) World's second largest container shipping company msc suffers a network outage, possibly due to a cyber attack. 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/

Centre for Risk Studies UniversityofCambridge (2019) Cambridge Global Risk Index 2019: Executive Summary. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-global-risk-index-execsummary-2019.pdf

De Smidt G, Botzen W (2018) Perceptions of corporate cyber risks and insurance decision-making. Geneva Pap Risk Insur Issues Pract 43(2):239–274

For Risk Studies CC (2019) Shen attack: Cyber risk in asia pacific ports. https://www.msig-asia.com/sites/msig_asia/files/downloads/CyRiM_ShenAttack_FinalReport.pdf

Goldsmith J (2013) How cyber changes the laws of war. Eur J Int Law 24(1):129–138

Grasso MI (2020) US Tugboat cyber-attack: the experts respond. https://www.ship-technology.com/features/cyber-attacks-in-the-maritime-sector-the-experts-respond/

Healey J (2017) Who's in control: Balance in cyber's public-private sector partnerships. Geo J Int'l Aff 18:120

Hubbard DW (2020) The failure of risk management: Why it's broken and how to fix it. John Wiley & Sons, New York

Hussain A, Kuhn K, Shaikh SA (2020) Games for cybersecurity decision-making. In: HCI-Games: 2nd international conference on HCI in games. Springer. In–press

International Transport Forum (2019) Itf transport outlook 2019. https://doi.org/10.1787/transp_outlook-en-2019-en

International Maritime Organisation (2020) 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. https://twitter.com/IMOHQ/status/1311601524209049601/photo/1. Tweet: 1311601524209049601
Jalali MS, Siegel M, Madnick S (2019) Decision-making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment. J Strat Inf Syst 28(1):66–82. https://doi.org/10.1016/j.jsis.2018.09.003, http://www.sciencedirect.com/science/article/pii/S0963868717304353
Jungmann SM, Witthöft M (2020) Health anxiety, cyberchondria, and coping in the current covid-19 pandemic: Which factors are related to coronavirus anxiety? J Anxiety Disord 102239:73
Kamphake AG (2020) Digitalization in controlling. In: Digitization in controlling. Springer, pp 3–25
Konrad J (2020) IMO Cyber-attack has serious implications. https://gcaptain.com/imo-cyberattack-has-serious-implications/
Kuhn K, Kipkech J, Shaikh S (2020) Maritime ports and cybersecurity vol. (In-press), pp (In–press). Institution of Engineering and Technology, United Kingdom
Lallie HS, Shepherd LA, Nurse JR, Erola A, Epiphaniou G, Maple C, Bellekens X (2020)
Lété B, Pernik P (2017) EU-NATO cybersecurity and defense cooperation: From common threats to common solutions german marshall fund of the United States
Lohrmann D (2020) 2020: The year the COVID-19 crisis brought a cyber pandemic. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html
Maliszewska M, Mattoo A, Van Der Mensbrugghe D (2020) The potential impact of COVID-19 on GDP and trade: A preliminary assessment. World Bank Policy Research Working Paper 9211
Malynn K (2020) Damage limitation following a cyber-security breach. https://www.rivieramm.com/recent-events/recent-events/maritime-cyber-riskmanagement-forum
Markit I (2020) Safety at Sea and BIMCO cyber security white paper. https://cdn.ihsmarkit.com/www/prot/pdf/1020/Safety-at-Sea-and-BIMCO-Cyber-Security-White-Paper-2020.pdf
Marsh LLC and Microsoft (2019) 2019 global cyber risk perception survey. https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf
Miró-Llinares F., Moneva A (2019) What about cyberspace (and cybercrime alongside it?) A reply to Farrell and Birks Did cybercrime cause the crime drop? Crime Sci 8(1):12
National cyber security centre (2020) Uk and allies expose russian attacks on coronavirus vaccine development. https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development
North Atlantic Treaty Organisation (2020) Partners. https://www.nato.int/cps/en/natohq/51288.htm
North Atlantic Treaty Organization (2010) Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf
North Atlantic Treaty Organization (2020) Statement by the north atlantic council concerning malicious cyber activities. https://www.nato.int/cps/en/natohq/official_texts_176136.htm
Eleftherios Ouzounoglou (2021) Cyber-mar: An innovative simulation environment. World of Shipping Conference 2021, January 28-29, 2021, virtual. https://www.cyber-mar.eu/wp-content/uploads/2021/02/WORLDO1.pdf
Pandey N, Pal A et al (2020) Impact of digital surge during covid-19 pandemic: A viewpoint on research and practice. Int J Inf Manag 102171:55
Papadopoulos T, Baltas KN, Balta ME (2020) The use of digital technologies by small and medium enterprises during COVID-19: Implications for theory and practice. Int J Inf Manag 55:102192
Pranggono B, Arabo A (2020) COVID-19 pandemic cybersecurity issues. Internet Technology Letters 4(2):e247
Reynolds Z (2020) Toll Logistics hit by second cyber attack. https://safetyatsea.net/news/2020/cyber-crimes-land-second-hit-on-toll-logistics/
Rogers GO (1984) Residential proximity, perceived and acceptable risk. In: Low-probability high-consequence risk analysis. Springer, pp 507–520
Shaikh SA (2017) Future of the sea : Cyber security. Foresight, Government Office for Science. London United Kingdom
Shapira Z (1995) Risk taking: A managerial perspective. Russell Sage Foundation
Shen C, Baker J (2020) CMA CGM confirms ransomware attack. https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack

Smith J, Doody K, Veitch B (2019) Being prepared for emergencies: a virtual environment experiment on the retention and maintenance of egress skills. WMU J Marit Aff 18(3):425–449
Stern E (2014) Designing crisis management training and exercises for strategic leaders: A Swedish and United States Collaborative project. National Defense College
Tam K (2020) What are the cyber threats to shipping? https://www.plymouth.ac.uk/news/pr-opinion/keeping-the-fleet-sailing-during-covid-19
Thunstrom L, Newbold S, Finnoff D, Ashworth M, Shogren JF (2020) The benefits and costs of flattening the curve for covid-19. SSRN 3561934
Twining G (2020) IMO hit by 'sophisticated' cyber attack. https://safetyatsea.net/news/2020/the-imo-hit-by-sophisticated-cyber-attack/
Twining G (2020) MSC confirm malware attack. https://safetyatsea.net/news/2020/msc-confirm-malware-attack/
Walker G, Simmons P, Wynne B, Irwin A (1998) Public perception of risks associated with major accident hazards. HSE contract research report
Weinstein D (2019) America's cyber blind spot. https://thehill.com/opinion/cybersecurity/461452-americas-cyber-blind-spot
Wiese Bockmann M (2019) Seized uk tanker likely 'spoofed' by iran. https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran
Williams MJ (2008) NATO, security and risk management: from Kosovo to Khandahar Routledge
ACI Worldwide (2020) Global eCommerce retail sales up 209 percent in April. https://www.aciworldwide.com/news-and-events/press-releases/2020/may/globalecommerce-retail-sales-up-209-percent-in-april-aci-worldwide-research-reveals
Xiang Z (2018) From digitization to the age of acceleration: On information technology and tourism. Tour Manag Perspect 25:147–150
Yam L (2021) Technology will help maritime transport navigate through the pandemic—and beyond. https://blogs.worldbank.org/transport/technology-will-help-maritime-transport-navigate-through-pandemic-and-beyond