2023

Ship's Cyber Security: Antecedents to improve Resilience Capabilities and their Impact on Decision-making and Collaborative Performance

Carine Dominguez-Péry

Kenza Arab

Céline Perea

Rana Tassabehji

SHIP'S CYBER SECURITY: ANTECEDENTS TO IMPROVE RESILIENCE CAPABILITIES AND THEIR IMPACT ON DECISION-MAKING AND COLLABORATIVE PERFORMANCE

Research full-length paper

Dominguez-Péry Carine, Univ. Grenoble Alpes, Grenoble INP, CERAG, 38000 Grenoble, France, carine.dominguez-pery@univ-grenoble-alpes.fr

Arab, Kenza, Univ. Grenoble Alpes, Grenoble INP, CERAG, 38000 Grenoble, France, kenza.arab@univ-grenoble-alpes.fr

Péréa, Céline, Univ. Grenoble Alpes, Grenoble INP, CERAG, 38000 Grenoble, France, celine.perea@univ-grenoble-alpes.fr

Tassabehji, Rana, University of Bath, Bath, United Kingdom, rt892@bath.ac.uk

Abstract

The maritime industry is made up of a complex ecosystem consisting of many actors. Digitalization has presented solutions to many earlier challenges faced by maritime professionals and has also led to new opportunities for improving maritime safety, vessel coordination, navigation, control, and communication. However, with these technological advances, have come new known and unknowable cyber-threats and cyber-security challenges to an industry that is already renowned for being one of the sectors most targeted by pirates and criminals. This study aims to investigate whether (and how) maritime safety culture and cyber-security factors (hygiene) impact on-board ship safety measured through maritime professionals' resilience capabilities, decision-making performance, and collaborative performance. The empirical findings of our quantitative study found that maritime professionals working onboard digitalised ships with improved awareness of cyber-security and the safety culture improved the overall resilience capabilities of ships and that onboard decision-making impacted collaboration with stakeholders.

Keywords: Cyber-Security Hygiene, Resilience, Collaborative Performance, Decision-Making Performance, Mari-time Ecosystems, Digital Systems, Maritime transportation

1 Introduction

Advances in new technologies, increased digitization of systems and the ever-increasing volumes and accessibility of big data are providing countless opportunities for transforming organizations and whole industry sectors. This is particularly true for the maritime industry, which has a complex ecosystem of entities (such as, port authorities, pilots, port and terminal infrastructures, multi-modal interfaces, incident response systems, on-board and onshore navigation aids, on-board information, and communications systems, etc.) that must interact effectively to ensure the safe and efficient operations of their maritime vessels (Michel and Noble, 2008). To date, the maritime transportation industry has benefited greatly from these technological advances to facilitate and improve navigation through increased automation, new electronic devices, radio, and satellite communication systems to name a few (Chacon, 2017).

However, these rapidly advancing technologies simultaneously presenting opportunities for more and further innovations and improvements, also expose industry actors to new and yet unidentified threats (Senarak, 2021a, b). For instance, while automation can make a considerable contribution to the reduction of maritime accidents, the system is complex and involves 'vessel control systems,' 'digital connectivity from vessel to shore,' and 'shore-based systems' (Cassauwers, 2020), all of which must be compatible, reliable, and secure. This inevitably means that any implementation of new digitized systems and technologies, especially in new contexts, are potentially more vulnerable to unpredicted and unpredictable cyber-attacks (Kavallieratos and Katsikas, 2020).

Cyber-attacks are defined as the unauthorized access to digital systems and (cyber)-networks with the intention of destroying and causing damage, disruption, obstruction and/or alteration to digital infrastructure, services or systems including networks, information computer systems, programs, and data motivated by external actors intending to do serious harm for personal, commercial, political, or national reasons (Alcaide and Llave, 2020). These attacks can take many forms, such as penetration, hijacking, cessation, and denial of services, and are conducted for the purposes of electronic warfare, military trickery, malicious intent, economic and commercial gain with multi-dimensional consequences (legal, economic, social, and technical) (Li & Liu, 2021).

In the maritime context in particular, there is an increase in the number of (cyber) terrorist attacks and there is a need for further research into the impact and implications of these attacks in a sector that has such a complex and inextricably linked ecosystem (Senarak,2021a, b; Kechagias et al., 2022).

According to a Cyber Risk Management (CyRiM) report, the measurable financial damage done by a single computer virus infecting only 6 ports could amount to $40.8 billion rising to $109.8 billion if 15 ports are affected (Daffron, 2019) resulting directly from business interruptions and loss of ser-vices and indirectly from the after-effects of damage to reputation, costs of recovery and longer-term losses in productivity and trust across the maritime ecosystem. As the extent of such losses have been described as "roughly equivalent to half of all losses from natural catastrophes globally in 2018" (Lloyd's of London, 2019), it is imperative that organisations operating within the maritime ecosystem and in particular maritime vessels, have in-built and established resilience capabilities in order to at best prevent and at worst minimise and quickly recover from the damage and disruptions of attempted cyberattacks Indeed policy makers recognise the importance of 'cyber resilience' - 'the ability for organisations to prepare for, respond to and recover from cyberattacks and security breaches' - as the key to operational resilience and business continuity and are working to implement policies to support organisations improve 'cyber resilience' (DSID, 2023).

However, research covering organisational resilience capabilities has been labelled as "promising" but "divergent" and "disjointed" (Kantur & İşeri-Say, 2012) and empirical studies on maritime organisational resilience are scarce with a call for more research into the factors that might lead to better resilience in maritime organisation (Akpinar & Özer-Çaylan, 2023). Furthermore, organisational resilience theory and practice would benefit greatly from developing a better and deeper understanding and conceptualisation of organisational resilience in particular its impact on decision-making, collaboration, and ultimately organisational performance. In this case of an increasing complex maritime ecosystem,

where various organisations must make joint decisions, collaborate, and interact in ways that directly and indirectly affect a wider global supply chain decision-making and collaboration are two fundamental components in the success of organisational 'performance' in this context.

This study therefore aims to gain an empirical and deeper insight into the role of cybersecurity 'hygiene' factors on organisational resilience capabilities, decision-making and collaborative performance as a means of improving overall cybersecurity. For this study, we applied a quantitative sur-vey methodology, to collect data from a sample of maritime professionals. Using structural equation modelling, our findings showed that cyber security hygiene factors influence resilience capabilities in the maritime context, which in turn leads to better decision-making collaborative performance. The remainder of this paper presents a brief overview of the literature, summarises methodology used for the data collection and analysis, and presents the findings of this exploratory study with conclusions and recommendations for future work. Our empirical study contributes to the organisational resilience literature by shedding light on the role of organisational resilience in the maritime context and its role in decision making and collaborative performance which is ever-more critical in ensuring the safety and security of ships at the centre of complex maritime ecosystems.

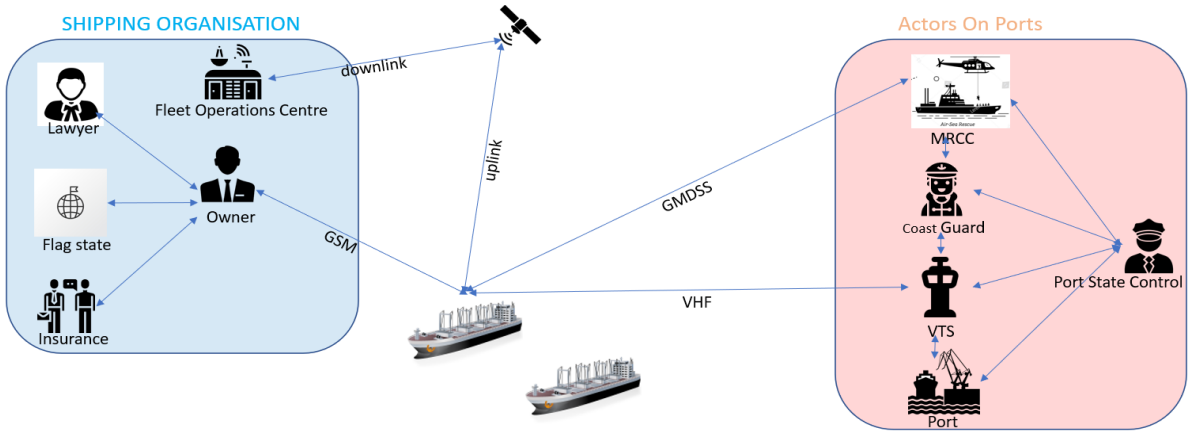
2 Digitalization of Ships in the maritime ecosystem

Maritime transportation is an information-intensive sector with different and complex data and information needed for a myriad of complex operations and tasks that take place across a range of different entities and stakeholders in the maritime ecosystem to ensure the efficient operations and safety of vessels (Watson et al., 2021b). Digital information systems and tools enable ships to perform operations such as, scene perception and navigation control (e.g., Electronic Chart Display Information System and High-Definition Cameras), energy efficiency analysis (e.g., attitude sensors), data transmission, reception, and processing (e.g., voyage data recorder and wireless communication systems), automatic obstacle avoidance (e.g., decision-making routing optimisation systems) (Zhang et al., 2021).

This digitalization is based on Information Technology (IT) and Operational Technology (OT) Systems. These are closely interlinked systems of hardware and software for processing information (IT) and directly monitoring and controlling physical devices and processes (OT) related to vessel navigation and management (Zăgan and Raicu, 2019; Androjna et al., 2020). Although both IT and OT are inextricably linked, they tend to remain siloed where IT departments are responsible for IT systems and specialized mechanical engineers are responsible for OT systems. This division of responsibilities is potentially problematic as both IT/OT systems are used to control navigation, engines, dynamic positioning, ship-to-shore interfaces, control of propulsion systems or opening and closing of cargo valves, passenger boarding systems (Alcaide and Llave, 2020:552). Consequently, integrated decision-making and close collaboration between the respective systems and decision-makers is critical for safe, effective, and efficient operations.

Some of the different actors and IT/OT systems that facilitate onboard-onshore communications and decision-making are illustrated in *Figure 1*. Some examples of this include, (i) ship owners that have fleet operation centres controlling the day-to-day operations of their fleet providing instructions to ships through internal systems or GSM (ii) the ships keeping in direct contact with port authorities or coast guards through the Vessel Traffic Service (VTS) or Maritime Rescue Co-ordination centres (MRCCs) in case of emergencies. Despite the need for regular multi-stakeholder interactions, the current state of the maritime ecosystems can be described as self-organized (Watson et al., 2021a:18) as there is no central point of control, which is largely distributed between different entities and stakeholders in the ecosystem at various times and under certain circumstances (for example in an emergency the coast guard takes control). Thus, currently, communication occurs under loosely coupled organizations, where actors come together to systematically adapt to events with no established or well-identified process. Consequently, closer integration of operational, communication and information management systems between stakeholders in the maritime ecosystem also creates new interdependencies and risks (Alcaide and Llave, 2020: 552). Within the maritime transportation industry, Global Navigation Satellite Systems (GNSS) and Automatic Identification Systems (AIS) have al-

ready been recognised as serious sources of digital vulnerabilities, as have low levels of awareness about information security (Lysne Utvalget, 2015), which will be discussed in more detail in the next section.



GMDSS - Global Maritime Distress and Safety System
GSM - Global System for Mobile Communications
MRCC - Maritime Rescue Coordination Centre
NGO - Non-governmental organization
VHF - Very high frequency
VTS - Vessel Traffic Service

Figure 1. Ships and Interconnection of Stakeholders in the Maritime Transportation Ecosystem (Source: Authors).

3 Security and Safety of Maritime Information Systems

Security and safety are critical in the maritime transportation industry (Kuntze et al., 2015; Line et al., 2006). Safety "relates to a system's inability to affect its environment in undesirable ways" (Line et al., 2006) and where accidents are rarely 'malicious' (Ghena et al., 2014). Consequently, the safe-ty of information systems is related to an internal analysis of risks in order to protect life, health, and the natural environment from damage (Line et al., 2006) by ensuring the system always returns to a safe state (Kuntze et al., 2015). On the other hand, security relates to a system's ability to operate in an orderly way even under external malicious threats (Ghena et al., 2014; Line et al., 2006). Information systems security aims to protect the confidentiality, integrity, and availability (CIA) of the information stored in and used by the system (Line et al., 2006). Thus, here we argue that security measures can also be a sub-set of safety measures because security incidents are increasingly causing safety incidents (Kuntze et al., 2015).

As the maritime industry becomes increasingly reliant on digitalization, integration of operations, and automation, there is a need to document and develop a deeper understanding of the potential digital vulnerabilities or cyber-risks and for the development of preventive and protective measures (Zăgan et al., 2018). According to the International Maritime Organization (2020), maritime cyber-risks are "*a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised*".

In 2018, 120 significant maritime OT system hacks were reported, which grew to 310 in 2019 (Marine Insight, 2020). Furthermore, since 2019, the shipping industry has become one of the seven most targeted industries with phishing campaigns (APWG, 2022). In 2021, in recognition of this increasing danger, the IMO requires ship owners and executives to include cyber-risk management in their ship safety protocols or run the risk of having their ships detained (IMO, 2020). In a review of the types of maritime cyber-risks highlighted in the literature, four major types of cyber threats and seven cyber-

vulnerabilities were identified, which are summarised in ***Erreur ! Source du renvoi introuvable.*** and categorised according to the area of vulnerability and intent.

In addition to the category and types of cyber-vulnerabilities we also highlighted the diverse groups willing and able to exploit maritime cyber vulnerabilities and launch cyber-attacks, which range from the individual to nation states from the literature (North, 2019). Each group has their motivations and objectives, which have been usefully categorized by the maritime insurer North (2019). However, it is important to note that the ultimate consequences of cyber-attacks are dependent on the targeted systems (Akpan et al., 2021) and the cyber-security measures they have implemented. North's (2019) categorization of groups engaging in intentional cyber-attacks and the consequences of those cyber-attacks highlighted in the literature, is summarized in Table 2.

3.1 Cyber-security in shipping

Cyber-security is a complex issue in that it has to be based on a myriad of processes, human psychosocial factors and motivations, and technical infrastructures and systems within organizations (Mraković and Vojinović, 2019). The human factor is fundamental in any cyber-attack as threats can arise intentionally from insiders who, might having access to the OT and/or IT systems or unintentionally exposing organisational systems to external threats through poor planning, lack of diligence, ignorance, or human error (Hadlington, 2021). Humans are also central to any cyber-security measures implemented to mitigate the risks of cyber-attacks (Meland et al., 2021; Tam and Jones, 2018). Thus, in order to effectively implement information security controls, there is a fundamental need to establish an information security culture where all individuals in the organization are made fully aware of security issues including how to recognise them, how to take the necessary precautions and report any breaches (Sasse and Flechais, 2005; Von Solms, 2006) and must be trained in cyber-security and risk response procedures (Mraković and Vojinović, 2019). For years, organisations have been exploring how best to engender an effective information security culture where appropriate security practices are embedded into working practices and well-integrated into organisational processes (Furnell, 2007). In an age of automation and digitisation, this has become even more of an imperative for the marine transportation industry.

To date, there have been several approaches published to identify cyber-threats in the maritime context. Kavallieratos et al. (2018) proposed the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) method for identifying cyber-threats based on a multi-level analysis of a ship's technological components, which examines the impact of a threat from an individual component to its wider parent and family of components. Using this method, Automatic Identification Systems (AIS), the Electronic Chart Display and Information System (ECDIS), and the Global Maritime Distress System (GMDSS) were identified as the most vulnerable of systems in marine transportation, with the most dangerous threats being Denial of Service (DOS) and Spoofing attacks (Kavallieratos et al., 2018).

In order to address these cyber-risks and vulnerabilities and minimize the impact of cyber-attacks, maritime vessels have been recommended to implement well-established technical security measures, such as setting up firewalls, intrusion detection and biometric authentication (Pfleeger and Caputo, 2012; Reddy and Reddy, 2014; Silverajan et al., 2018). Furthermore, maritime professionals need to prioritise how they limit and control access to their networks, protocols and services while also implementing an automatic detection, blocking, and warning process throughout their systems (Yoo and Park, 2021). There is also a need to establish clear and consistent information systems security management policies, practices, and procedures for all the entities and stakeholders operating within the maritime ecosystem (Mraković and Vojinović, 2019), in line with good security practice enshrined in the ISO/IEC 27001 information security management standard (www.iso.org). In addition to these recommendations, raising awareness of and training in information security onboard and onshore was ranked as the highest priority by maritime professionals, followed by technical and administrative measures (Yoo and Park, 2021).

Category	Types of cyber-threats	Types of cyber vulnerabilities	References
Human	• Unintentional: Lack of training and expertise in cybersecurity matters, • Intentional*: Hacktivists, criminal, and terrorist groups targeting	• Lack of stakeholder control over industrial systems.	(Schröder-Hinrichs, 2010; Heij and Knapp, 2018; Ahokas, 2019; BIMCO, 2019; Park et al., 2019; Benham and Sproule, 2017).
Technical	• Unintentional: The use of outdated IT and OT systems.	• Lack of secure development, • Low level of access protection, • The lack of partitioning between IT and OT systems, • Increasing use of unsecured standard computer systems.	(Sen, 2016; Jones et al., 2016; Park et al., 2019; Benham and Sproule, 2017),
Process	• Intentional: The introduction of malicious software through personal devices*.	• The absence of abnormal supervision of the system, • Out-of-date and weak management protocols.	(Teoh and Mahmood, 2018: Fayi, 2018; Park et al., 2019; Benham and Sproule, 2017).
*Intentional Attacks: 1) Digital piracy by shutting down the vessel/port; 2) Extortion/ransomware to restore vessel/port operations; 3) Espionage for gaining sensitive information that can be used by the competition/nation states; 4) Subversion of the supply chain; 5) Terrorism; 6) Activism to convey a message.			Androjna et al. (2020)

Table 1. Cyber threats and vulnerabilities in the shipping industry.

Group*	Motivation*	Objective*	Consequences	References
Activists (including disgruntled employees)	• Reputational damage • Disruption of operations	• Destruction of data • Publication of sensitive data • Media attention	• Data theft and/or destruction, • Ship hijackings, • Disruption of vessel operations, • Loss of communication, • Compromising computers, • Loss of lives and cargo, • Change of GPS coordinates, • Physical damage to facilities, • Unplanned shutdowns, • Financial damage, • Reputation damage.	Ukwandu et al., 2022 ; Androjna et al., 2020 ; Meland et al., 2021 ; Tam and Jones, 2019 ; Kessler et al., 2018 ; Oxford Analytica, 2019 ; Kavallieratos et al., 2018 ; Svilicic, Brčić et al., 2019 ; Wu et al., 2018 ; Pavur et al., 2020 ; Alcaide and Llave, 2020 ; Shoultz, 2017 ; Caprolu et al., 2020).
Criminals	• Financial gain • Commercial espionage • Industrial espionage	• Selling stolen data • Ransoming stolen data • Ransoming system operability • Arranging fraudulent transportation of cargo		
Opportunists	• The challenge	• Getting through cyber security defences • Financial gain		
• Nation States • State sponsored organizations • Terrorists	• Political gain • Espionage	• Gaining knowledge • Disruption to economies and critical national infrastructure		

*Table 2. Actors of cyber-attacks, their motivations, objectives, and consequences (*Adapted from North and based on BIMCO (2016))*

While establishing preventative cyber-security measures and monitoring are fundamental to the overall safety and security of maritime vessels, cyber-resilience, the ability to prepare and recover from cyber-attacks, is equally important (Kleij and Leukfeldt, 2019). Organisational cyber-resilience builds and improves anticipatory and monitoring abilities, reduces incident response times, increases the ability to learn after each attack, and is emerging as a critical capability for organizations to deal with potential and actual cyber-attacks more effectively (Kleij and Leukfeldt, 2019). Policy makers, cyber-security practitioners and researchers are increasingly focusing on developing effective tools and frameworks to support organizational cyber-resilience, for instance by measuring the number of attempted and successful cyber-attacks, through more rapid tracking, tracing, and fixing of breaches and their wider impact on organisational operations (Accenture, 2021a, 2021b).

Having established the need to address new and serious cyber-risks and cyber-attacks within the maritime transportation industry, and to seamlessly integrate cyber-security into the well-established and deeply embedded safety culture of the maritime industry, in what follows, this study proposes how this might be done.

4 Theoretical Framework

To address the aims of this study, we propose an empirical model to identify the relationship be-tween safety, security, and resilience in the maritime transportation industry from the perspective of maritime professionals. Here, we first develop the hypotheses that will form the basis of our theoretical model which includes (i) identifying the extent to which safety climate and cyber hygiene influence resilience capabilities (ii) how resilience capabilities influence decision-making performance and ultimately (iii) how these influence collaborative performance, which is so critical in the complex maritime ecosystem.

4.1 Resilience Capabilities: Influence of safety climate and cyber-security

Resilience was first introduced by Holling (1973) to comprise both recovery and adaptive capabilities; in the context of social sciences, the concept of resilience describes the behavioural responses of groups, national economies, and systems to recover their regular operations in a flexible, responsive, and timely manner when faced with adversity (Ponomarov and Holcomb, 2009). Organisational resilience is a multi-dimensional concept comprising of main three dimensions (Trinh et al., 2019; Pillay et al., 2010): (i) cognitive resilience which includes the interpretation and analysis of un-known situations, (ii) behavioural resilience which facilitates the full use of organisational resources and routines enabling it to learn and implement new routines, and (iii) contextual resilience which consists of interpersonal networks, spare resources and lines of supply that would enable an organisation to take quick actions under risky and uncertain circumstances. More recently, resilience capabilities have been defined as a system's capacity to withstand changes in the environment with agility, flexibility, and speed (Yang et al. 2018). In the maritime context, as we have already established, resilience is fundamental to safety onboard and onshore and research has already found that resilience capabilities in shipping operations lead to a reduction in the number of accidents and cargo damage (Gligor et al., 2015; Lee and Rha, 2016; Yang et al., 2018).

In the context of maritime transportation, a safety culture incorporates the many roles and responsibilities, actions, and values to ensure the well-being of the vessel, its cargo and crew at all times. A safety climate is a snapshot of safety that captures the attitudes and perceptions towards safety (its practices and management) at a specific point in time (NIOSH, 2022). In our study, we focus on the safety climate of navigation from the perspective of maritime professional. We posit that Safety Climate, which is the awareness and endorsement of best safety practices, contributes to improving organisational resilience against unintentional and accidental hazards but also for also for intentional and malicious exploitation of cyber-threats through cyber-attacks. Thus, we hypothesise that:

H1: **Safety Climate positively influences Resilience Capabilities of ships.**

Cyber-resilience increasingly plays a critical role in minimising the impact of cyber-attacks and maximising the ability to recover from them (Kleij and Leukfeldt, 2019; IT Gouvernance, 2017). In the maritime context, little is known about the constituents of resilience capabilities and cyber-resilience in particular, which we address here. By embedding an organisation-wide cyber-security and safety climate, this helps organisations and their employees to better understand what and how critical events (accidents, incidents, and hazards) happen and their consequences, as well as making available organisational resources, including human resources and cyber-security measures and processes, that can help mitigate the probability of these events happening (Casey et al., 2017; O'Connor et al., 2011; Zohar, 2010) and ultimately impact organisational resilience (Mraković and Vojinović, 2019).

Cyber-security is undoubtedly associated with resilience capabilities and can be considered as a way to encourage users to adopt safe and secure behaviours online (Pfleeger et al., 2014). Indeed, Vishwanath et al. (2020) identify cyber-security hygiene as a means of improving cyber-resilience. In this context, cyber-security hygiene means using cyber-security 'best practices', including technology, behaviour, and processes, to protect and maintain systems and devices connected to the Internet (Almeida et al., 2017; Mraković and Vojinović, 2019), which is fundamental to organisations operating in the maritime transportation sector. In one of the few studies investigating the extent to which cyber-security hygiene impacts individual and group cyber-resilience in the maritime ecosystem, Senarak (2021a) operationalised the measure for cyber-hygiene (CHI) which covers five largely technical dimensions (storage and devices, transmission, social media, authentication credential, emails, and messaging). We adapt these measures here and posit that cyber-security hygiene will impact the resilience capabilities of a maritime organization.

H2: **Cyber-Security Hygiene positively influences Resilience Capabilities of ships.**

4.2 The Impact of Resilience Capabilities on Decision-Making Performance

In the maritime context, we have argued that organizational resilience is the ability not only to survive attacks and accidents, but also to have the ability to solve problems in the face of disruption, and more importantly to be able to proactively track, trace and identify the problems before they escalate into more serious incidents (Akpinar & Özer-Çaylan, 2023). In an increasingly digitised and turbulent environment, in order to survive and thrive, it is critical for maritime organisations to be able to build the type of organisational resilience where informed decisions are made based on a holistic scan of the environment taking into account the different outcomes of the decisions to be taken (Akpinar & Özer-Çaylan, 2023). Indeed, studies have shown that resilience capabilities improve the efficiency of decision-making (Grafton et al., 2019) and the need for more novel resilience-based decision-making to better manage increasingly complex systems (Salomon et al., 2020).

Indeed, measures of organizational resilience (recovery, response, learning) are an ever-critical part of strategic planning and decision-making (Phillips and Chao, 2022). Thus, in the context of an increasingly digitized, complex, and inter-connected maritime ecosystem, there is a need for seamless decision-making – that is accurate, effective, and efficient and incorporates resilience measures. In this study, we have identified decision-making performance as accuracy, timeliness (Speier et al., 2003), effectiveness and efficiency of decision-making (Visinescu et al., 2017; Shamim et al., 2020).

Finally, resilience consisting of in better preventing and detecting false data, will facilitate the final decision-making on board. This is particularly true for spoofing cyber risks in maritime. It is when the satellite signal or location address is compromised through the internet in order to present false positional data and information thereby positioning the entity in a different position other than its real position. Pirates are using spoofing tools like virtual private networks and shields bought on the internet to direct ships to danger zones before being hijacked, thereby increasing the number of spoofing incidents in the maritime industry. In addition, Bhatti & Humphreys (2017) demonstrated the vulnerability of ships to false Global Positioning System (GPS) (spoofing).

Consequently, we posit that when an organisation engages in policies and establishes procedures that foster resilience, it will improve organisational processes and make them more flexible, responsive,

and quick to recover when faced with disruptions. Thus, our third hypothesis is that Resilience Capabilities improves decision-making performance:

H3: **Resilience Capabilities positively influences Decision-Making Performance.**

4.3 The Impact of Decision-Making performance on Collaborative Performance

Earlier, we argued that effective collaboration is critical in the overly complex environment of maritime transportation ecosystems, and so there is a need to understand how to improve collaborative performance in the context of maritime decision-making. This is even more important knowing that there are asymmetries of information between the captain and its crew on ship and the stakeholders on shore. For instance, ships can see other ships that are close to them whereas these ships will not be visible on shore if the AIS device of certain ships is off. Conversely, stakeholders on ports may have more information than a ship on the potential causes of a cyber-attack by analysing data coming from multiple ports and/or sites? These asymmetries of information highlight the necessity to improve the collaboration between stakeholders on sea and on shore.

Within the maritime sector, decision-making tends to be built on the established naval command and control where the captain of the ship is the law and legally the ultimate decision-maker (Aragon & Messer, 2001). Consensus is an important component of maritime command and control, where variations in outcomes and their effectiveness in stress situations, are based on the variations in decision-making disagreement (Perry and Moffat, 1997) - once a decision is made by the commander in control, there is a need to achieve consensus through collaboration with other stakeholders.

Taking into account the modern-day complexities of the maritime industry and the various stakeholders with potentially distinct types of complementary information, it is even more important to ensure that there is a shared view of operations for critical decision-making (MITAGS, 2023). Consequently, we have included collaborative performance as a measure of achieving consensus in the context of the relationships among the different entities and stakeholders in a partnership shared resources (information, systems, processes, expertise, and infrastructure) and work closely in order to design, implement and fulfil their operational objectives (Krishnan et al., 2006). A study by Kim and Oh (2005) concluded that optimal collaborative performance is dependent on the partners' ability to set the right objectives for their collaboration and their ability to equally accommodate perspectives through collaboration once the commander makes the decision. So here we posit that in the maritime context, the performance of decision-making on ships will positively influence the decisions made by both the ship and stakeholders on shore to enact accurate, timely and objective-oriented decisions. Thus, our fourth hypothesis is:

H4: **Decision Making Performance positively influences Collaborative Performance.**

5 Methodology

Our study purposely targeted professional mariners who had experience of management and navigation onboard ships to take part in our survey. The survey instrument was made available via the Le Sphinx online platform and distributed to a professional group of crew members on LinkedIn, with experience of the following roles: Captain, Chief engineer, Deck Officer, Chief Officer, Second Engineer, Junior Deck officer, Junior chief officer, Junior Engineer, Deck rating, engine rating, Seafarer. The onboard roles were selected based on our exploratory interviews and pre-tests with experienced professionals and using information gathered from specialized websites such as Seamanmemories[1] and

[1] https://www.seamanmemories.com/

the Jubilee Sailing Trust[2]. The survey was targeted at respondents that were onboard or onshore at the time of the survey, but those onshore had to be included in the survey, those onshore had to have at least some experience in navigation onboard. Data was collected over a 5-week period, where 875 crew members were contacted, and sixty-nine responded with a 7.88% response rate. Although this is seemingly sparse number; it is notoriously difficult to reach active and experienced maritime professionals because of the nature of their work which involves prolonged periods at sea and the difficulties of access.

The survey consisted of several sections – one that collected general profile and descriptive statistics of the respondents (such as age, gender, role, years of experience, etc.) and the constructs built from the hypotheses already posited above. In our survey, we adapted measurement instruments from studies, not related specifically shipping industry. Safety climate is a second order construct built on four dimensions, the other four constructs (Resilience Capabilities, Cyber Security Hygiene, Decision-making Performance, and Collaborative Performance) are first order constructs. They all are considered as constructs with reflexive items.

For our predictive and explorative study, following Hair et al. (2011) we applied Structural Equation Modelling techniques using PLS (Partial Least Squares) to build and evaluate our model using R language and the SEMinR package developed by Hair et al. (2021). Following the guidelines of Hair et al. (2021) and of Kante and Michel (2023), we assessed the reliability, the validity of scales and the model quality.

6 Results

Table 3 summarises the profiles of our sample of respondents based on the descriptive statistics collected.

Statistic	Modality	Frequency	Statistic	Modality	Frequency
Size of Company	Small	21.74%	Roles on board	Captain	33.33%
	Medium	53.62%		Chief Engineer	13.04%
	Large	24.64%		Second Engineer	1.45%
Continent of origin	Africa	5.80%		Junior Engineer	4.35%
	Asia	11.59%		Chief Officer	11.59%
	Europe	69.59%		Junior Chief Officer	1.45%
	North America	8.70%		Deck Rating	4.35%
	South America	4.35%		Deck Officer	13.04%
				Junior Deck Officer	2.90%
				Other	10.14%

Table 3. Sample descriptive statistics.

In evaluating the measurement model, we kept items with factor loadings higher than the threshold of 0.708. All AVE values exceed the threshold of 0.5, and all Composite Reliability (CR) indices are greater than 0.6. The constructs' internal consistency, reliability and convergent validity is presented in *Table 4*. All the results of the outer model are presented. Discriminant validity was confirmed through the Heterotrait-Monotrait (HTMT) values, which are all significantly lower (90% percentile bootstrap Confidence Interval) than the threshold value of 0.90 (Hair et al., 2021) (summarised in **Erreur ! Source du renvoi introuvable.**).

[2] https://jst.org.uk/

Construct	Item-dim	Loadings	Cronbach's α	Composite Reliability	AVE
Safety Climate	SaCli_commi	0.71	0.782	0.860	0.607
	SaCli_Commu	0.88			
	SaCli_supp	0.80			
	SaCli_info	0.71			
Resilience Capabilities	RSL1	0.76	0.879	0.908	0.623
	RSL2	0.83			
	RSL3	0.82			
	RSL4	0.79			
	RSL5	0.78			
	RSL6	0.75			
Cyber Security Hygiene	CySec1	0.92	0.956	0.963	0.765
	CySec2	0.91			
	CySec3	0.86			
	CySec4	0.85			
	CySec5	0.86			
	CySec6	0.88			
	CySec7	0.86			
	CySec8	0.84			
Decision-making performance	DPERF1	0.94	0.883	0.944	0.895
	DPERF2	0.95			
Collaborative Performance	CPERF1	0.85	0.889	0.922	0.748
	CPERF2	0.89			
	CPERF3	0.89			
	CPERF4	0.83			

Table 4. Constructs' validity and reliability.

The results of the Structural Equation Modelling (***Erreur ! Source du renvoi introuvable.*** and ***Erreur ! Source du renvoi introuvable.*** validated all the hypotheses of our model. In the Discussion session, we first comment on the upstream part of the model (relationships between safety climate, cyber security hygiene with resilience capabilities) (7.1) and then the downstream part of our model in section (7.2).

Considering the model quality, we relied on the VIF value of 1.394, which is largely below the threshold of five. Therefore, collinearity among independent variables is not a critical issue in our model. Our model's explanatory power (R^2) is quite good: as it explains more than 47% of the variance in resilience capabilities, 9% in decision-making performance, and 35% in collaborative performance. Common method bias was evaluated by computing the Harman's single-factor which is adapted in PLS-PM models (Kock, 2020). The AVE of the single factor is below the threshold of 0.5 showing a value of 0.303 here. Thus, common method bias is not an issue here.

7 Discussion

7.1 The antecedents of resilience capabilities in navigation shipping

In terms of investigating the antecedents to Resilience Capabilities onboard ships, this construct was found to be influenced both by Safety Climate and Cyber Security Hygiene. Safety Climate relates to the perception of the safety climate, including information security. It measures management openness, safety concerns and the quality of shared information among the crew. Resilience Capabilities

measures the capacity to detect changes, threats and risks related to ships as well as the capacity to be flexible and responsive when facing challenges or during the recovery phase after incidents and/or accidents. Cyber Security Hygiene measures cyber-attacks and threats detection and prevention abilities by ship systems and crew members. In addition to internal efficiency, and the ability to oversee and communicate about cyber-attacks, this construct also encompasses the quality of communication with the ships' external collaborative networks with actors in ports (e.g. VTS or the coast guard) and within the ship company onshore (as per *Figure 1*), which extends the work of You et al. (2017), Senarak (2021a,b) and Tam et al. (2021). The whole management involvement in safety concerns, the quality of information sharing and communication both internally and with the whole maritime ecosystem promotes a resilient behaviour of the ship when faced with adversity and hazards (e.g., cyber-threats or attacks). Furthermore, the relationship between Cybersecurity Hygiene and Resilience Capabilities can be linked to the way good cybersecurity hygiene practices (both human and technical) contribute to improving resilience and further consolidates the taxonomy of Johnsen and Kilskar (2020) who presented resilience in cybersecurity as encompassing elements such as design, engineering, and communication.

As shown in *Figure 2*, Safety climate is the construct that most influences Resilience Capabilities (path: 0.525) in comparison to Cyber Security Hygiene (path: 0.249). Safety Climate reflects a well-established safety culture that has been fostered in the maritime industry over centuries as opposed to Cyber Security Hygiene, which is a relatively new and emerging concern in the industry. The main novelty emerging from these results is the combination of cyber security hygiene and safety climate as antecedents of organisational resilience capabilities, as previous studies have either focused exclusively on safety climate and safety culture or cyber security hygiene, without linking them to other organisational constructs.

7.2 The role of resilience capabilities to explain decision making and collaborative performance.

The downstream part of the model (*Figure 2*) relates to the influence of resilience capabilities on decision-making and collaborative performance. Decision-making is related to decisions on board whereas Collaborative Performance (CPERF) relates to the collaboration between the ship and the shore, which is becoming increasingly more critical with the advancing digitalisation of ships and related maritime ecosystem.

In our finding that Resilience Capabilities positively influence Decision-Making Performance, we posit that a prominent level of resilience capabilities implies that organisations have improved their processes and communication modes which will inevitably positively influence decision-making processes to make responses to changes and hazards, timelier and more effective. Moreover, Decision Making Performance (DPERF) is mainly related to the ability to detect risks, threats or any changes that may impact onboard safety in an accurate, timely and result-oriented way. Complementary, CPERF is related to the collaboration between the ship and the stakeholders onshore and measures mutual satisfaction between the ship and actors in the whole maritime ecosystem, notably onshore partners based in ports. When decision-making is approached through results-orientation, accuracy, and timeliness it leads to building relationships that are objective-oriented, clear, and stable over time, where all actors are working collaboratively to improve their operational safety and policies to reduce risks. Hence, an initial DPERF onboard led by the captain is necessary to instigate and improve an effective CPERF.

8 Conclusion

8.1 Theoretical contributions

This quantitative study is one of the very few studies to empirically investigating the link between cybersecurity and other organisational constructs. According to many authors, maritime cybersecurity literature is still underdeveloped (Park et al., 2019; Mraković and Vojinović, 2019; de la Peña Zarzuelo, 2021). To our knowledge, the studies of Senarak (2021a and b) are the only ones developed in the maritime context with a survey on cyber risks. Thus, the constructs used in our survey measurement are adapted from other industries such as the aviation.

Our study highlights the need for maritime resilience capabilities to improve safety including cyber threats and attacks. Improving onboard navigation processes and behaviours, improves overall safety and directly impacts resilience capabilities. Thus, actively developing efficient cyber risk management strategies and practices should be an integral part of the overall safety climate of ships, including the management of outsourced third parties.

Another main result is the need to consider equally the importance of the role actors onboard and onshore must play throughout the whole maritime ecosystem, to effectively prevent and/or respond to cyber threats and risks in a timely and efficient way, through communication and collaboration.

8.2 Managerial Implications

This study confirms and extends the roles involved to better prevent or fight against cyber risks in the maritime context (BIMCO, 2019). Fighting and preventing cyber risks should be considered more holistically in the organisation, not only by those with direct links and competencies in information technologies or systems all stakeholders to improve navigation safety and resilience capabilities targeting cyber risks. Moreover, Cyber Security Hygiene should figure as part of the safety culture components onboard ships, where all crew members should receive training in cyber risks mitigation and cyber security measures in case of attacks.

Finally, by increasing the resilience of the whole maritime ecosystem, including the ship and shipping company, to cyber risks, the more they will be able to detect and react to them building knowledge to improve decision-making. This is key considering the speed at which cybercriminals are able to develop and execute new types of cyber threats and attacks.

8.3 Limitations and future work

To the best of our knowledge, this research is one of the few that has investigated cybersecurity in ships and the impact on organisational resilience capabilities, decision-making performance, and collaborative performance. One of the main limitations is the size of our sample and response rate. However, as this is an exploratory study, it is our intention to build further on this study and build our networks in the industry to improve our response rates. Other limitations concern the analyses of the model which can be extended. We still need to exploit data to highlight control variables such as the level of experience of respondents, their position (onshore or onboard) and their roles. Finally, we intend to further develop this research by investigating cybersecurity practices and policies onboard and in ports with qualitative data to highlight what works well and the current barriers, which will complement this study.

HTMT	SaCli	CySec	RSL	DPERF	CPERF	SaCli_Commi	SaCli_commu	SaCli_supp	SaCli_info
SaCli									
CySec	0.613								
RSL	0.773	0.571							
DPERF	0.363	0.332	0.346						
CPERF	0.404	0.471	0.534	0.658					
SaCli_commi		0.485	0.470	0.321	0.355				
SaCli_commu		0.566	0.753	0.323	0.442	0.826			
SaCli_supp		0.483	0.711	0.112	0.168	0.601	0.898		
SaCli_info		0.482	0.631	0.446	0.340	0.434	0.573	0.835	

Table 5. HTMT values.

Hypothesis	Path Coeff	T stat.	2.5% CI	97.5% CI	Support
H1 SaCli → RSL	0.525	5.787	0.377	0.729	Yes***
H2 CySec → RSL	0.249	2.372	0.030	0.437	Yes*
H3 RSL → DPERF	0.307	2.703	0.075	0.520	Yes**
H4 DPERF → CPERF	0.593	7.274	0.421	0.739	Yes***
Bilateral test. ***p < 0.001 “3.107”; **p < 0.01 “2.586”; *p < 0.05 “1.965” 95% percentile bootstrap Confidence Interval with 10,000 bootstrap subsamples					

Table 6. Direct effects.

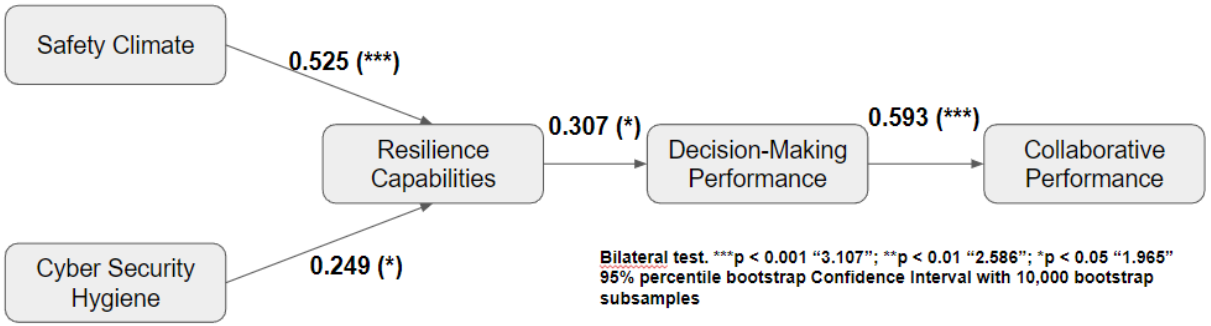


Figure 2. Theoretical Model with path coefficients.

References

Accenture, 2021a. The state of cybersecurity resilience 2021 – How aligning security and the business creates cyber resilience. Available online (accessed on Oct 31st, 2022): https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

Accenture, 2021b. The state of cybersecurity resilience 2021. Available online (accessed on Oct 31st, 2022): https://www.accenture.com/us-en/insights/security/invest-cyber-resilience

Ahokas, I. (2019). The Finnish maritime sector and cybersecurity. *Publications of the HAZARD Project*. https://blogit. Utu. Fi/hazard, retrieved.

Akpinar, H., & Özer-Çaylan, D. (2023). Organizational resilience in maritime business: a systematic literature review. *Management Research Review*, 46(2), 245-267.

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, 45, 547-554.

Almeida, V. A., Doneda, D., & de Souza Abreu, J. (2017). Cyberwarfare and digital governance. *IEEE Internet Computing*, 21(2), 68-71.

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*, 8(10), 776.

APWG (2022). Phishing Activity Trends Reports. Available Online (accessed on Nov 13th, 2022): https://apwg.org/trendsreports/

Aragon, J R.; Messer, T.A. (2001). Master's handbook on ship's business. *Cambridge, Md: Cornell Maritime Press*. ISBN 0-87033-531-6.

Bhatti, J., & Humphreys, T. E. (2017). Hostile control of ships via false GPS signals: Demonstration and detection. N AVIGATION, *Journal of the Institute of Navigation*, 6 4 (1), 51-66.

BIMCO (2016). Guidelines on Cyber Security Onboard Ships V1. Available at (Accessed on Oct 20th, 2022): https://www.nepia.com/guidelines_on_cyber_security_onboard_ships_version_1-1_feb2016/

BIMCO (2019). The Guidelines on Cyber Security Onboard Ships. Bimco. Available Online (Accessed on Oct 20th, 2022) : https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Caprolu, M., Di Pietro, R., Raponi, S., Sciancalepore, S., & Tedeschi, P. (2020). Vessels cybersecurity: Issues, challenges, and the road ahead. *IEEE Communications Magazine*, 58(6), 90-96.

Casey, T., Griffin, M. A., Flatau Harrison, H., & Neal, A. (2017). Safety climate and culture: Integrating psychological and systems perspectives. *Journal of occupational health psychology*, 22(3), 341.

Cassauwers, T. (2020) Automated shipping coming to Europe's waters. Horizon, The EU Research & Innovation Magazine Available from https://ec.europa.eu/research-and-innovation/en/horizon-magazine/automated-shipping-coming-europes-waters

Chacon, V.H. (2017). The New Technologies Applied in Maritime Transportation. In: The Due Diligence in Maritime Transportation in the Technological Era. *Springer Series on Naval Architecture, Marine Engineering, Shipbuilding and Shipping*, vol 5. Springer, Cham. https://doi.org/10.1007/978-3-319-66002-8_4

Daffron, 2019. Shen attack cyber risk scenario: up to $110 billion at risk from maritime malware attack. Link (accessed on June 25th, 2023): https://risk-studies-viewpoint.blog.jbs.cam.ac.uk/2019/10/30/shen-attack-cyber-risk-scenario-up-to-110-billion-at-risk-from-maritime-malware-attack

De la Peña Zarzuelo, I. (2021). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. *Transport Policy*, 100, 1-4.

DSID (2023) Cyber resilience: Details of the government's cyber resilience policy for businesses and organisations. Department for Science, Innovation and Technology and Department for Digital, Culture, Media & Sport 12 April 2023 Available from https://www.gov.uk/government/collections/cyber-resilience Accessed 20/6/23

Fayi, S. Y. A. (2018). What Petya/NotPetya ransomware is and what its remediations are. In *Information technology-new generations* (pp. 93-100). Springer, Cham.

Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., & Halderman, J. A. (2014). Green lights forever: Analyzing the security of traffic infrastructure. In *8th USENIX workshop on offensive technologies (WOOT 14)*.

Gligor, D. M., Esmark, C. L., & Holcomb, M. C. (2015). Performance outcomes of supply chain agility: when should you be agile?. *Journal of operations management*, 33, 71-82.

Grafton, R. Q., Doyen, L., Béné, C., Borgomeo, E., Brooks, K., Chu, L., Cumming, G. S., Dixon, J., Dovers, S., Garrick, D., Helfgott, A., Jiang, Q., Katic, P., Little, L. R., Matthews, N., Ringler, C., Squires, D., Steinshamn, S. I., Villasante, S., Wheeler, S., Williams & J., Wyrwoll, P. (2019). Realizing resilience for decision-making. *Nature Sustainability*, 2(10), 907-913.

Hadlington, L. (2021). The "human factor" in cybersecurity: Exploring the accidental insider. In *Research anthology on artificial intelligence applications in security* (pp. 1960-1977). IGI Global.

Hair, J. F., Hult, T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). Partial least squares structural equation modeling (PLS-SEM) using R: A workbook. *Springer*.

Heij, C., & Knapp, S. (2018). Predictive power of inspection outcomes for future shipping accidents–an empirical appraisal with special attention for human factor aspects. *Maritime Policy & Management*, 45(5), 604-621.

Holling, C.S., 1973. Resilience and stability of ecological systems. Annu. Rev. Ecol. Syst. 4, 1–23.

IMO (2020). Maritime cyber risk Available online (Accessed on Oct 20th, 2022): https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

IT Gouvernance (2017). What is cyber resilience. Available online (accessed on Oct 31st, 2022): https://www.itgovernance.co.uk/cyber-resilience

Johnsen, S. O., & Kilskar, S. S. (2020). A review of resilience in autonomous transport to improve safety and security. In *Proceedings of the 30th European Safety and Reliability Conference*.

Jones, K. D., Tam, K., & Papadaki, M. (2016). Threats and impacts in maritime cyber security.

Kante, M., & Michel, B. (2023). Use of partial least squares structural equation modelling (PLS-SEM) in privacy and disclosure research on social network sites: A systematic review. *Computers in Human Behavior Reports*, 100291.

Kantur, D., & İşeri-Say, A. (2012). Organizational resilience: A conceptual integrative framework. *Journal of Management & Organization*, 18(6), 762-773.

Kasim, H., Hassan, C. R. C., Hamid, M. D., Emami, S. D., & Danaee, M. (2018). Determination of factors affecting safety practices in Malaysian radiation facilities. *Safety science*, 104, 70-80.

Kavallieratos, G., & Katsikas, S. (2020). Managing cyber security risks of the cyber-enabled ship. *Journal of Marine Science and Engineering*, 8(10), 768.

Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2018). Cyber-attacks against the autonomous ship. In Computer security (pp. 20-36). *Springer*, Cham.

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, 37, 100526.

Kessler, G. C., Craiger, J. P., & Haass, J. C. (2018). A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 12(3), 429.

Kim, B., & Oh, H. (2005). The impact of decision-making sharing between supplier and manufacturer on their collaboration performance. *Supply Chain Management: An International Journal*.

Kleij, R. V. D., & Leukfeldt, R. (2019, July). Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security. In *International conference on applied human factors and ergonomics* (pp. 16-27). Springer, Cham.

Kock, N. (2020). Harman's single factor test in PLS-SEM: Checking for common method bias. *Data Analysis Perspectives Journal*, 2(2), 1-6.

Krishnan, R., Martin, X., & Noorderhaven, N. G. (2006). When does trust matter to alliance performance? *Academy of Management journal*, 49(5), 894-917.

Kuntze, N., Rudolph, C., Brisbois, G. B., Boggess, M., Endicott-Popovsky, B., & Leivesley, S. (2015, April). Security vs. safety: Why do people die despite good safety?. In *2015 Integrated Communication, Navigation and Surveillance Conference (ICNS)* (pp. A4-1). IEEE.

Lee, S. M., & Rha, J. S. (2016). Ambidextrous supply chain as a dynamic capability: building a resilient supply chain. *Management Decision*.

Li, X., Goldsby, T.J., Holsapple, C.W., 2009. Supply chain agility: scale development. Int. J. *Logist. Manage*. 20 (3), 408–424.

Li, Y., Liu Q., (2021) A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports 7* (November 2021): 8176-8186

Line, M. B., Nordland, O., Røstad, L., & Tøndel, I. A. (2006, May). Safety vs security?. In *PSAM Conference*, New Orleans, USA. Sn.

Lloyd's of London, 2019. Single cyber-attack on Asia-Pac ports could cost $110bn, equal to half of all 2018 natural disasters. Link (accessed on June 25th, 2023): https://www.lloyds.com/about-lloyds/media-centre/press-releases/cyber-attack-on-apac-ports-could-cost-110bn

Meland, P. H., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 15.

Michel, K., Noble, P. (2008) Technological Advances in Maritime Transportation The Bridge, 38 (2), Available from https://www.nae.edu/19579/19582/21020/7419/7712/TechnologicalAdvancesinMaritimeTransportation#about_author7712 Accessed 1/11/2022

MITAGS (2023) Critical Decision-Making in the Maritime Industry – Maritime Institute of Technology & Graduate Studies Online Available from https://www.mitags.org/critical-decision-making/ accessed 10/6/2023

Moshtari, M. (2016). Inter-organizational fit, relationship management capability, and collaborative performance within a humanitarian setting. *Production and Operations Management*, 25(9), 1542-1557.

Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis–how to reduce threats?. *Transactions on maritime science*, 8(01), 132-139.

NIOSH (2022) Overlap and difference between safety culture and safety climate. Available from https://www.cdc.gov/niosh/z-draft-under-review-do-not-cite/safetyculturehc/module-1/5.html Accessed 28/4/2022

North (2019). Cyber Risks in Shipping. Available at (Accessed on Oct 20th, 2022): https://www.nepia.com/identifying-cyber-threats/

O'Connor, P., O'Dea, A., Kennedy, Q., & Buttrey, S. E. (2011). Measuring safety climate in aviation: A review and recommendations for the future. *Safety Science*, 49(2), 128-138.

Oxford Analytica. (2019). Global maritime security risks rise with GNSS use. *Emerald Expert Briefings*, (oxan-db).

Park, C., Shi, W., Zhang, W., Kontovas, C., & Chang, C. H. (2019). Cybersecurity in the maritime industry: A literature review. In *20th Commemorative Annual General Assembly, AGA 2019-Proceedings of the International Association of Maritime Universities Conference*, IAMUC 2019 (pp. 79-86).

Pavur, J., Moser, D., Strohmeier, M., Lenders, V., & Martinovic, I. (2020, May). A tale of sea and sky on the security of maritime VSAT communications. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 1384-1400). IEEE.

Perry, W., Moffat, J. Measuring consensus in decision making: an application to maritime command and control. *J Oper Res Soc***48**, 383–390 (1997). https://doi.org/10.1057/palgrave.jors.2600372

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, 31(4), 597-611.

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, 11(4), 489-510.

Phillips, F. Y., & Chao, A. (2022). Rethinking Resilience: Definition, Context, and Measure. *IEEE Transactions on Engineering Management*.

Pillay, M., Borys, D., Else, D., & Tuck, M. (2010). Safety culture and resilience engineering–exploring theory and application in improving gold mining safety. *Gravity Gold*, 21, e2.

Ponomarov, S.Y., Holcomb, M.C., 2009. Understanding the concept of supply chain resilience. *Int. J. Logist. Manage*. 20 (1), 124–143.

Reddy, G.N.; Reddy, G. A study of cybersecurity challenges and its emerging trends on latest technologies. arXiv 2014, arXiv:1402.1842.

Richard Benham and James Sproule. Cyber Security. IOD Policy Report March, (March): 177, 2017.

S. Furnell, "IFIP workshop – Information security culture," *Comput. Secur*., vol. 26, no. 1, p. 35, Feb. 2007.

Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it?. *O'Reilly*.

Schröder-Hinrichs, J. U. (2010). Human and organizational factors in the maritime world—Are we keeping up to speed?. *WMU Journal of Maritime Affairs*, 9(1), 1-3.

Sen, R. (2016). Cyber and information threats to seaports and ships. *Maritime Security*, 281-302.

Senarak, C. (2021a). Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel. *The Asian Journal of Shipping and Logistics*, 37, 345-360.

Senarak, C. (2021b). Port cybersecurity and threat: A structural model for prevention and policy development. *The Asian Journal of Shipping and Logistics*, 37(1), 20-36.

Shamim, S., Zeng, J., Khan, Z., & Zia, N. U. (2020). Big data analytics capability and decision making performance in emerging market firms: The role of contractual and relational governance mechanisms. *Technological Forecasting and Social Change*, 161, 120315.

Shoultz, D. (2017). Securely Connected Vessels: Vessel Communications and Maritime Cybersecurity. Accessible online (accessed on Oct 20th, 2022) : https://www.maritimeprofessional.com/blogs/post/securely-connected-vessels-vessel-communicationsandmaritime-15176.

Silverajan, B.; Ocak, M.; Nagel, B. Cybersecurity attacks and defences for unmanned smart ships. In *Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, 30 July–3 August 2018; pp. 15–20.

Speier, C., Vessey, I., Valacich, J.S., 2003. The effects of interruptions, task complexity, and information presentation on computer-supported decision-making performance. *Decision Sciences* 34 (4), 771–797.

Svilicic, B., Brčić, D., Žuškin, S., & Kalebić, D. (2019). Raising awareness on cyber security of ECDIS. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 13(1).

Tam, K., & Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18(1), 129-163.

Tam, K., & Jones, K. D. (2018). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, 3(2), 147-164.

Tam, K., Moara-Nkwe, K., & Jones, K. (2021). The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training. *Maritime Technology and Research*, 3(1), Manuscript-Manuscript

Teoh, C. S., & Mahmood, A. K. (2018). Cybersecurity workforce development for digital economy. *The Educational Review*, USA, 2(1), 136-146.

Trinh, M. T., Feng, Y., & Mohamed, S. (2019). Framework for measuring resilient safety culture in Vietnam's construction environment. *Journal of construction engineering and management*, 145(2), 04018127.

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., ... & Bellekens, X. (2022). Cyber-security challenges in aviation industry: a review of current and future trends. *Information*, 13(3), 146.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, 128, 113160.

Visinescu, L.L., Jones, M.C., Sidorova, A., 2017. Improving decision quality: the role of business intelligence. *J. Computer Information Systems* 57 (1), 58–66.

Wang, Q., Kayande, U., & Jap, S. (2010). The seeds of dissolution: Discrepancy and incoherence in buyer–supplier exchange. *Marketing Science*, 29(6), 1109-1124.

Watson R.T., Lind M., Delmeire N., Liesa F. (2021a), "Shipping: a self-organising ecosystem", In Maritime informatics (pp. 13-32). *Springer*, Cham.

Watson, R. T., Haraldson, S., Lind, M., Rygh, T., Singh, S., Thomas, D., ... & Ward, R. (2021b). FOUNDATIONS OF MARITIME INFORMATICS. In *2021 World of Shipping Portugal. An International Research Conference on Maritime Affairs 28-29 January 2021*, Online Conference, from Portugal to the World.

Wu, Z., Pan, Q., Yue, M., & Ma, S. (2018, August). An Approach of Security Protection for VSAT Network. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 1511-1516). IEEE.

Yang, C. C., & Hsu, W. L. (2018). Evaluating the impact of security management practices on resilience capability in maritime firms—a relational perspective. *Transportation Research Part A: Policy and Practice*, 110, 220-233.

Yoo, Y., & Park, H. S. (2021). Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. *Journal of Marine Science and Engineering*, 9(6), 565.

You, B., Zhang, Y., & Cheng, L. C. (2017, May). Review on Cyber Security Risk Assessment and Evaluation and Their Approaches on Maritime Transportation. In *Proceedings of the 30th Annual Conference of International Chinese Transportation Professionals Association*, Houston, TX, USA (pp. 19-21).

Zăgan, R., & Raicu, G. (2019). Understanding of the cyber risk on board ship and ship stability. *Annals of" Dunarea de Jos" University of Galati*. Fascicle XI Shipbuilding, 42, 81-90.

Zohar, D. (2010). Thirty years of safety climate research: Reflections and future directions. *Accident analysis & prevention*, 42(5), 1517-1522