Cruising Digitalization

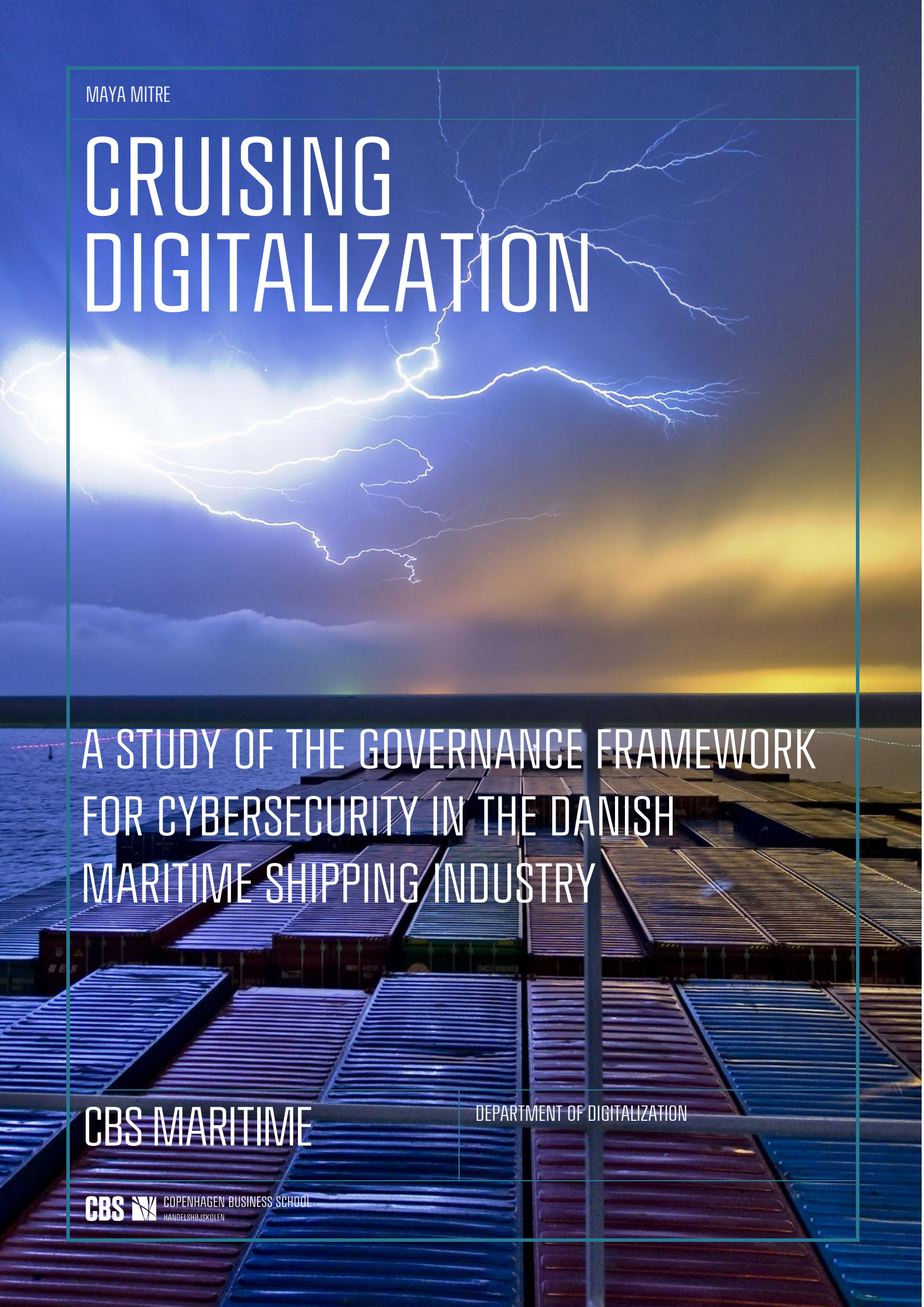
A Study of the Governance Framework for Cybersecurity in the Danish Maritime Shipping Industry

Mitre, Maya

MAYA MITRE

CRUISING DIGITALIZATION

A STUDY OF THE GOVERNANCE FRAMEWORK FOR CYBERSECURITY IN THE DANISH MARITIME SHIPPING INDUSTRY



CBS MARITIME

DEPARTMENT OF DIGITALIZATION

CBS COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

PUBLISHED BY:
CBS MARITIME
FEBRUARY 2020

CBSMARITIME@CBS.DK
WWW.CBS.DK/MARITIME

FRONT PAGE PHOTO:
IRIS/SCANPIX

PRODUCTION:
CBS MARITIME

GRAPHIC PRODUCTION:
CBS MARITIME

CONTENTS

EXECUTIVE SUMMARY

This report is the result of a one-year research project, which investigates the adequacy of the current governance framework for cybersecurity in the maritime shipping industry using Denmark as a main reference. More specifically, the report discusses the roles of technology, regulation and self-regulatory schemes in building a governance framework to ensure cyber security within maritime shipping. It departs from the question of whether it makes sense to regulate cybersecurity in shipping, at the industry level, considering that shipping organizations themselves are the main beneficiaries of cyber hygiene or cyber resilience. In the process of exploring this and related questions we have consulted reports, applicable regulation, and policies at the national and supranational levels, interviewed key stakeholders in the Danish shipping industry, and participated in relevant events. On a general level, we conclude that the superposition of regulatory and self-regulatory structures, combined with the use of technology, are indispensable for providing cyber resilience, taking into account particularities of the industry and of cybersecurity itself. Given current technological developments in the field of digitalization, which connect information technology (IT) and operational technology (OT) in shipping, cybersecurity is now closely associated with ship safety, thus making regulation necessary and the insertion of cybersecurity into the ISM code adequate. Still, one should not discount the importance of guidelines provided by industry actors, which account for the layer of self-regulation. Finally, although technologies, such as artificial intelligence (AI), play a vital role in preventing cyber threats, their main contribution lies in directing human behavior towards desirable outcomes – for example, by enforcing the use of strong passwords. This reaffirms the principle that the main tool in fighting cyber threats continue to be human beings themselves. It is to that extent that we propose, as a tool for **"cruising digitalization"**, that shipping organizations establish a clearer connection between the safety of information systems and ship safety. In this line, we suggest that, similarly to other health and safety issues, cyber resilience should be framed as an issue of social responsibility in the maritime shipping industry, and a priority issue for top management, and for each and every employee. In a country such as Denmark, which prides itself of its high level of digitalization, and for whom the shipping industry is paramount, this becomes furthermore an opportunity to increase the level of identification between shipping organizations and their employees, and to increase the proximity between the goals of the industry and those of the Danish society.

INTRODUCTION

Despite general claims concerning the maritime shipping industry's low permeability to innovation and high attachment to tradition, its digital transformation is now conspicuous. As the use of internet of things (IoT) sensors powered by artificial intelligence (AI) and machine learning within vessels allows for the profuse generation, collection, and processing of digital data, new business models are being created, and traditional sources of revenue are becoming obsolete[1]. In the same vein, progress in AI and robotics are pushing prototypes of automated and unmanned ships to a whole new level, while blockchain solutions connect the supply chain without need for intermediaries[2].

This high dependence on computerized systems and information and communication technologies, and the fact that most vessels are now permanently connected to the internet can, however, be met with yet another type of disruption, besides the disruption of traditional businesses models: namely the stalling of, or interference with, shipping operations due to cyber incidents. It is also in this sense that cruising digitalization, a metaphor we use in allusion to a smooth adaption to digital technologies, can become a challenge.

In the last couple of years, several regulatory actions targeted at increasing the maritime shipping industry's cyber resilience, or reducing cyber threats, have been taken. Most notably, the International Maritime Organization (IMO), through its Maritime Safety Committee has adopted a resolution requiring administrations to ensure that cyber risks are addressed in safety management systems[3]. Additionally, the committee approved guidelines on maritime cyber risk management, thus alerting to the importance of the integrity of information systems to the vessel's safety and security[4].

At the regional level, these regulatory pieces connect with the European Union's Directive on Security of Network and Information Systems (NIS Directive)[5] and to some extent with the well-known General Data Protection Regulation (GDPR)[6]. At the Danish (national) level, which is the focus of this report, they are associated with the Danish Maritime Authority's 2019 Cyber and Information Security Strategy for the Maritime Sector, a sub-strategy within the Ministry of Finance's broader Danish Cyber and Information Security Strategy of 2018[7].

The above listed regulatory efforts have been complemented by a series of self-regulatory initiatives on the part of industry actors. Most notably, BIMCO, together with other industry organizations, have released in 2018 the third version of their guidelines on cyber security on board ships, which are considered as a good parameter by national organizations[8].

Having this regulatory and policy context as background, this report sets out to explore the question of whether the current governance framework for cybersecurity in the maritime shipping industry is adequate. More specifically, we departed from the following questions:

Is there a need for regulating cybersecurity in the shipping industry? In other words, does it make sense to create and enforce rules upon the actors that seem to be the main beneficiaries of these rules – namely, maritime shipping organizations? Or would that amount to an unnecessary intervention by legislators in an instance where the market alone and/or technology are sufficient to reach the desired outcomes? Finally, in case regulation is necessary, what kind of governance framework is appropriate?

Without ignoring the global character of the industry, as well as the importance of the international regulatory structure and the supply chain, we attempt to answer these questions by focusing on Denmark. More specifically, we explore the Danish Shipping industry's current cybersecurity governance framework and its particularities.

[1] On this topic, see Danish Ship Finance and Rainmaking (2018), on the final references.
[2] On this topic, see Lloyd's Register et al. (2017), on the final references.
[3] Resolution MSC. 428 (98), adopted on 16 June 2017. See final references.
[4] Guidelines on Maritime Cyber Risk Management. Published on 5 July 2017. See final references.
[5] Directive on security of network and information systems. Adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. See final references. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[6] Regulation EU 2016/679 of the European Parliament and the Council. See final references. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[7] See final references.
[8] See final references.

As a result of this effort, we have come to a better understanding of the particularities of cybersecurity (within and outside shipping) and a deeper knowledge of the shipping industry itself. More specifically, the report concludes that the key for understanding the particular "governance model" adopted by the shipping industry (both in Denmark and globally) to tackle cybersecurity lies in the current interdependencies that exist between information technology (IT) and operation technology (OT). The blurring of boundaries between IT and OT also connects the integrity of information systems with the safety of vessels, passengers and crew, thus making cybersecurity a key point in allowing the industry to cruise digitalization. This connection, moreover, reinforces the need for international regulation, while not dispensing with self-regulatory schemes.

This report is divided in 7 sections. After this introduction, clarification of the methodology is provided: i.e., the types of sources consulted, as well as description of the research process. The section titled "Clearing the waters: what is cybersecurity?" initializes the "review of the literature" with a broad discussion on the meaning of cybersecurity. Here, there lies an attempt to make sense of the subject by clarifying the relationship between cybersecurity and information security, the areas to which cybersecurity applies, as well as differences in terms of perpetrators and motivations. We close with a brief discussion of cybersecurity from the perspective of externalities, which connects directly with the issue of regulation.

The fourth section (Regulation and self-regulation in the maritime shipping industry), which is the most extensive, marks our incursion into the field of shipping. More specifically, it starts with a historical and policy account of regulation in maritime shipping and then moves into more theoretical discussions on the effectiveness of alternative co-regulatory models in different industries, including shipping. It ends with a brief explanation of IMO's International Safety Management Code (ISM) and its relevance for cybersecurity. "The role of technology as a regulator", as the title suggests, briefly explores how technological advancements can be helpful in ensuring cybersecurity in general. "Cybersecurity in the Danish shipping industry: an exploratory study" is where the findings on the Danish shipping industry are presented and organized according to 4 subcategories or codes. The seventh section confronts the findings with the explored literatures, thus providing points for discussion. Here, the main limitations of this report are also acknowledged. Finally, the eighth and final part is devoted to conclusions and suggestions for future research.

METHODOLOGY

The contributions of this report are situated not only in its findings, but also in the way it attempts to promote a "dialogue" between different literatures and disciplines that are concerned either with cybersecurity, with regulation in the shipping industry, or both. This explains why this section (methodology) precedes the review of the literature. As mentioned, rather than crafting a more traditional review of the literature, we sought to interweave different literatures and disciplines that could contribute to the problem. More specifically, we consulted (1) a well consolidated literature on information security and cybersecurity in the field of information systems, (2) a literature that analyzes information security and cybersecurity from the perspective of economics, (3) a broad literature on self-regulation, which draws on institutional theory and policy studies, and (4) a specialized literature that analyzes regulation and safety regulation within shipping from either a historical or a regulatory perspective. We supplemented the review of journal articles and books with publications from media outlets, whitepapers (egg. from cybersecurity consultancies), position papers (egg. from the International Union of Marine Insurers), and reports from consultancies and diverse organizations within and outside shipping (egg. BIMCO, OECD, Lloyd's Register, Quinetiq and University of Southampton, Danish Ship Finance and Rainmaking, Danish Shipping, and Rambøll and Core).

When analyzing specifically the case of cybersecurity in shipping, and particularly the case of Denmark, we started by consulting a series of relevant policies and regulations. Thereafter, we collected primary data in two ways: first, by participating in two subscription-based events promoted by the shipping industry, and second, by interviewing experts. The first event, titled Cyber Security – threat landscape, trends and employee awareness, was organized by the Maritime Development Center in Denmark and took place in November 2018, at the University of Aalborg's campus in Copenhagen. It comprised of three lectures with the following specialists: Morten von Seelen, a senior manager at Deloitte's Cyber Incident Response, Ken Munro, a partner of Pen Tests Partners, and Kasper Hulgaard, a behavioral consultant and project manager at INudge You. These presenters shared their slides after the event, and we quote them accordingly.

The second event was the one-day course offered by the Danish Shipping Academy, titled Introduction to the Shipping Industry, hosted by Danish Shipping (Danske Rederier) in April 2019. The course had the format of several short lectures delivered by Danish Shipping staff occupying roles such as director, analyst, head of industrial relations, and head of legal affairs. Information based on notes from the course and shared slides (in print) are quoted as Danish Shipping 2019, and do not make reference to specific persons.

Finally, this primary data was supplemented by interviews with two cybersecurity specialists (one at a national shipping association and another at a private consulting company), a security specialist at an international shipping association, and a specialist in digitalization at a national shipping association. More specifically, in November 2018 a joint interview of approximately 45 minutes was conducted with Asbjørn Overgaard Christiansen, head of innovation and Danish Shipping Academy, and Morten Glamsø, senior adviser in the field of security, environment and maritime research, both at Danish Shipping (Danske Rederier). In December of 2018, Lars Jensen, a specialist in cybersecurity within shipping and founder of the consulting Cyberkeel (now part of Improsec Aps), shared his knowledge in an interview that lasted for one hour. Jensen had hosted and mediated the Maritime Development Center event on cybersecurity a month earlier, where a first contact with him was established. In April 2019 the opportunity of going to Bagsværd to meet Jakob Larsen, head of security at BIMCO, appeared, resulting in an interview of approximately 45 minutes. Finally, in May 2019, a follow up interview of approximately 40 minutes with Morten Glamsø concluded the process of primary data collection. All interviews were recorded with consent and direct quotes were sent to interviewees for purposes of validation.

After transcribing the interviews and looking at notes and other primary sources, findings were organized in accordance with the following codes: (1) regulation, self-regulation and accountability (2) safety, security, and the ISM Code, (3) information sharing, awareness and brand

sensitivity, (4) security by design, nudging, and the human factor. The process through which we arrived at these codes was both deductive and inductive. In other words, while codes such as “regulation and self-regulation” were extracted from the literature, and are what Saunders et al. (2016, 582) consider to be “a priori” codes, other codes were adapted or created after assessing the primary sources. These are known as “in vivo” codes (Saunders et al. 2016, 583) and offer a greater degree of flexibility. Finally, for purposes of problem delimitation, it is important to mention that the focus here is on cybersecurity within vessels, even though some of the consulted regulation go beyond vessels and cover port infrastructure.

CLEARING THE WATERS: WHAT IS CYBERSECURITY?

It is difficult to explain the meaning of cybersecurity without referring, first, to the concept of information security. Most definitions of information security refer back to the North-American Central Intelligence Agency's (CIA) benchmark model or triad created in the 1970s to assess the security of information. The triad emphasizes the need of ensuring that information preserves the properties of confidentiality (prevention of unauthorized access and/or disclosure), integrity (assurance that information is accurate, trustworthy and untampered) and availability (the guarantee that those who are authorized to access it may easily do it). The same parameters are reproduced in the 2013 ISO/IEC 27001 standard for information security management[9], as well as on the North-American NIST cybersecurity framework[10].

Contrarily to what some may assume, the concept of information security does not apply exclusively to digitally stored information. Moreover, it includes both physical and logical access controls to ensure "the proper use of data and to prohibit unauthorized or accidental modification, destruction disclosure, loss or access to automated or manual records and files as well as loss, damage or misuse of information assets" (Peltier 2001, 266). Since the end of the 1980s, however, a growing focus on digitally stored information started to arise, and the concept of information security evolved in consonance with digital information systems themselves, thus giving rise, as we will see below, to the concept of cybersecurity.

In 1992 the Organization for Economic Cooperation and Development (OECD) issued its first Recommendation Concerning Guidelines for the Security of Information Systems, directed at both national governments and the private sector. This report was based on the recognition that building trust in digital information systems was of absolute importance given their centrality for trade, as well as social, cultural, and social interactions. The paradigm of information security at that time was informed by the siloed infrastructure of information technology. Security thus "focused on internal threats", and protection against the "outside world" was gained through "reinforcing the main characteristics of information systems: keeping them closed by default and opening them only by exception and under tight controls" (OECD 2002, 5).

The so-called "age of perimeter security" (OECD 2012) of the early 1990s was swiftly replaced at the end of the same decade due mainly to the wide adoption of internet technologies. In this new environment, "seamless interoperability and interconnectivity enabled the various, previously siloed, IT components of organizations to morph into joined-up information systems, within which information could flow freely" beyond organizational and even national borders (OECD 2012, 6). The transformation of the IT infrastructure promoted by the internet, and the fact that "breaches of security resulting from attacks on data or systems via a connection to an external network or system" (Danish Ministry of Finance 2018, 7) were now able to occur gave way to an unprecedented expansion of economic and social interactions. On the other hand, new opportunities for crime also came to the fore, thus giving rise to the concept of cybercrime, to which cybersecurity is related.

One of the best means of understanding cybersecurity and thus analyzing different governance frameworks associated with it is by distinguishing the different meanings conflated in the term. One could start by differentiating among three broad areas to which cybersecurity may apply, namely, national security, industrial espionage and cybercrime. These areas "differ dramatically in terms of scale, stakeholders, timeframe and level of social importance" (Friedman 2011, 2).

Among the three areas, the case of "national security" is quite particular, as actions such as the disruption of a nation's critical infrastructure and attacks against the military are extraordinary situations, characterized by a high level of social importance, huge scale, very specific stakeholders (usually states and terrorist groups) and a complex timeframe calculus (Friedman 2011, 2).

In the cases of industrial espionage and cybercrime scale is hard to appraise. If we consider the former, it will become clear that "both governments and companies are understandably reluctant to disclose details, and thus figures are based on assumptions and informed judgments,

[9] https://www.iso.org/standard/54534.html

[10] https://www.nist.gov/cyberframework

rather than accurate numbers (Friedman 2011, 3). In the case of cybercrime, estimates suffer from the problem of a regular conflation of "risks with threats, harms and crimes" (Wall 2017, 1083)[11]. Usually, what we see in the media are estimates concerning risks and threats of cybercrime, which display the highest numbers but say little about actual harms to the victims. In spite of this tendency to "over-sensationalize", cybercrime may paradoxically go underreported, either because victims such as businesses prefer not to report them, or because they are prosecuted under different laws.

Regarding the level of social importance of cybercrime, it is important to keep in mind that the idea of "zero crime" is illusory, and that a certain level of fraud "has become a built-in expense in most business models that rely on the internet (Friedman 2011, 4). As a matter of fact, "there is a trade-off between fraud reduction and enabling transactions such as e-commerce", and both governments and businesses need to take in a certain marginal cost of attacks as the "cost of doing business" (Friedman 2011, 4). Specifically with regard to espionage, the idea of the long-term competitiveness of national industries should be considered, as the stealing of intellectual property might affect the long-term interests of companies, shareholders and society as a whole.

Different from Friedman, Wall (2017, 1081-1083) assesses cybercrime in accordance with three variables: (1) the importance of technology as a mediator, (2) the modus operandi, and (3) the victims. In order to measure the first variable he suggests a so-called "transformation test", which consists of metaphorically or actually "removing" the mediating technology from the crime in order to assess "what is left". The result could be any one of three different categories of crime: at the two opposite ends one would have either the cyber-assisted crime, which is the crime that profits from the internet but would still take place without its existence, or the cyber-dependent crime, which only exists because of the internet. In the category in between one could list a number of cyber-enabled crimes, which are "existing crimes in law" and which are now acquiring a more global nature due to the use of networked systems. The "modus operandi" variable, in turn, appraises whether a cybercrime was a "crime against the machine" (i..e an attack targeted at computer networks), a crime that "uses the machine" (i.e. fraud), or a "crime in the machine" (i.e., hate speech online). Finally, it is also important to differentiate among types of victims, which can be categorized into individuals, nation states and organizations.

A category that is not mentioned in any of the typologies above refers to perpetrators and their motivations. Von Seelen (2018) tackles this by listing the following perpetrators and pairing them up with common motivations: (1) criminals/ financial gain, (2) Hackers/ curiosity or fame, (3) Hacktivists/ affect public opinion or company behavior, (4) insiders/ disagreements or profits, (5) competitors / gain competitive advantage, (6) nation states / political and security concerns, and (6) accidents / accidental.

Depending on how one frames the problem, however, the category of "insiders" – with diverse or no motivation – encompasses all the others. This is the argument made by Arduin (2018). For him, regardless of the structure of information systems (i.e., whether they are siloed or networked) their main threat factor is "human and internal" (Arduin 2018, 62). This happens because while codes, procedures, and infrastructures are effective in protecting "computer systems", they are not sufficient in guaranteeing the security of "information systems" because the latter include a crucial and yet highly unpredictable component, namely, humans, or individuals, who may, or may not, behave rationally. Here it is important to understand that violations to organizational security policies can be of diverse nature, and the author distinguishes between three categories of violations (Arduin 2018, 65):

1) un-intentional, that is, "wrong actions" carried out unconsciously by employees either due to inexperience or negligence, or because they were manipulated by an attacker. An example here would be the deletion of sensitive data.

2) intentional and non-malicious, that is, wrong actions that are deliberately taken by employees, such as deferring updates and backups or choosing weak passwords, which are made with the purpose of derive a benefit (for example, saving time), but which have no intention to cause harm.

3) intentional and malicious, which refer to deliberate actions caused by employees with a desire to cause harm, such as divulging sensitive data.

The main aspect that distinguishes the first and second categories in this typology seems to be "unawareness" of policy violation. Regarding the second and third, the difference lies in the intention to cause harm, although the

[11] According to Wall (2018, 1083), risks are things that "in theory could happen, such as a meteorite that might destroy life on earth". Threats, in turn, "are those risks that are in circulation at any one time, such as meteorites flying around the cosmos but no necessarily hitting anything". Harms and crimes, however, are something of a different nature, since they actually refer to a violation of the law (crime) even if actual harm was not done.

intention to derive a benefit from the action (present in 2 but not always present in 3) may also contribute to making the second category blameworthy from a moral standpoint.

Arduin's (2018) insistence in the importance of the "human element" in ensuring information security is echoed by several other information systems scholars, who claim that a focus on technological solutions, system's components (software and hardware) and systems solutions is far from sufficient (see, for instance, Boss et al. 2009, Herath and Rao 2009). These scholars argue for the need to heed formal and informal control mechanisms, including policies, procedures, organizational culture, and the role individuals play in security (Herath and Rao 2009, 106, see also Pahnila et al. 2007). In other words, there is both the need to develop security policies (Dutta and McCrohan 2002) and to motivate individuals within the organization to comply. The latter usually requires a serious commitment on the part of management, and maybe even the perception on the part of individuals that their actions contribute to the organization.

For Boss et al. 2009, one of the variables that most contributes to ensuring cybersecurity is "mandatoriness", which refer to the degree to which "individuals perceive that compliance with existing security policies and procedures is compulsory or expected by organizational management" (Boss et al. 2009, 152). Among the findings of their study, one should highlight: (1) that acts of specifying policies and evaluating behaviors are effective in convincing individuals that security policies are mandatory, (2) that the perception of mandatoriness is effective in motivating individuals to take security precautions and, most importantly, (3) that if individuals believe that management is watching, they will comply.

The incentive of actors to engage in criminal behavior online are diverse. Still, the idea of creating destructive code just for the sake of disruption seems to be decreasing in what Wall (2017, 1079) calls a "post-script kiddie world". In other words, one should "model today's cybercriminal as an actor seeking some goal" (Friedman 2011, 6); not so much as a teenager performing a rite of passage. To that extent, the main incentives left are either financial or political. When speaking of the former one could refer to those engaged in "economy of scale" types of crime. Here, assisted by the automation of digital technologies, which are lowering the "entry level skills of cybercrime", criminals commit a large amount of small crimes, with an individual low return, but which also incur in lower risk of being caught and punished (Wall 2017, 1078-9). At a different level of gain lie crimes targeted at industrial espionage, intellectual property theft and similar issues. Finally, actors with non-financial or political incentives can be anything from "white hat" hackers and "hacktivists", to cyberterrorists, or someone who wants to harm a firm's reputation, even without deriving any financial gains from it.

While the incentives of engaging in cybercrime may be clear, incentives for enhancing cyber security at the individual or organizational level are a bit more complex, and thus invite the question of the extent to which regulation, or interference with the market, are necessary in this field[12]. Here, it is important to ask whether individual information security decisions reflect social benefits and costs, that is to say, if they result in an "overall desirable outcome" for society, which is "a tolerable level of cybercrime, a desirable level of security" (Bauer and Eeten 2009, 707). If some of the costs are borne by other stakeholders or some of the benefits accrue to other players (i.e., they are "externalized"), individual security decisions do not properly reflect social benefits and costs. Another way to put this is that "private network owners" do not completely internalize the risks of not protecting themselves adequately, nor do they completely internalize the benefits.

For Dourado and Britto (2012), although network security has positive externalities that private network owners cannot internalize, this does not amount to a market failure and, therefore, does not necessarily require governmental interference. For them, private firms, due to "self-interested reasons" are already investing a lot in security precautions and thus providing enough positive externalities. Therefore, there is no market failure and thus regulation is redundant.

Another means to appraise this scenario is by focusing on negative externalities (Bauer and Eeten 2009). In the case of highly interdependent information and communication systems such as the internet, although the security decisions of a market player regarding malware might be rational for that player, given the costs and benefits it perceives, the resulting course of action inadvertently or deliberately imposes costs on other market players and on society at large. Decentralized individual decisions will therefore not result in a socially "optimal level of security", and therefore require some regulatory interference. In other words, although one can see a number of instances in which "market-based incentive mechanisms that enhance security" are working, there are

[12] Here, it is important to notice that cybercrime and information security belong to two different, though interdependent, markets (Bauer and Eeten 20019, 717).

also instances in which decentralized actions are afflicted by externalities and thus suboptimal outcomes (Bauer and Eeten 2009, 713).

The idea of comparing cybersecurity with locking your own home (Dourado and Britto 2012) might not provide an accurate analogy here, as in this case there are not so many negative externalities, or at least they are not so direct. Alternatively, a comparison with vaccines and vaccination programs makes more sense (Mital 2015). In this case, there are positive externalities when individuals vaccinate (in the sense that non-vaccinated individuals are also protected by default) and, conversely, negative externalities when individuals refrain from doing so (to the extent that they may get sick and represent a social cost, as well as contaminate others). Similarly, "unvaccinated" computers represent substantial negative externalities associated with the potential and realized threat of millions of compromised PCs - thus the rationality of comparing cybersecurity with a "public health issue", which requires some degree of governmental interference or at least coordination (Mital 2015, 3).

Modeling cybersecurity as an economic problem will directly lead us into a discussion on regulation, which is the main focus of this report. After all, if a problem of collective action or a prisoner's dilemma type of situation is at stake, some sort of coordination might be important. In the next section, we approach the topic of regulation directly in reference to the maritime shipping industry.

REGULATION AND SELF-REGULATION IN THE MARITIME SHIPPING INDUSTRY

Globalization and global capitalism are far from new phenomena. And yet few industries can claim to have "global" inscribed into their DNA to the same degree as the maritime. Indeed, it was through technologies of navigation that globalization itself came into being: civilizations crossed oceans to come into contact with other ways of living, and capitalism and the nation-state as we know them today begun to take form.

The fact that the maritime industry is global and broad translates, among other things into a complex, multi-layered and at times juxtaposed regulatory structure. Regulation in the shipping industry combines the efforts of, on the one hand, political actors (egg. flag state administrations, port state authorities and international legislative bodies) and, on the other, private actors (classification societies, P&I clubs, trade unions, industry associations). These actors may, in turn, be based nationally/locally, regionally or internationally.

Maritime shipping, in particular, abounds with regulatory challenges, not the least because ships spend much of their time in international waters, outside of the reach of regulators (Almklov & Lamvik 2018, 176). For this reason, and given the global nature of the industry, the need for "international co-ordination" is conspicuous (Walters and Bailey 2013, 2009). It therefore makes sense that the bulk of relevant regulation in the shipping industry departs from the walls of the International Maritime Organization (IMO), a body of the United Nations that came into existence in 1958.

The history of regulation in the maritime industry refers back to XIX century England, and more specifically to the efforts of private actors. These actors were marine underwriters and brokers who, faced with increasing ship losses, and the need to manage risk, introduced a system of rating for ships, which in turn gave birth to the so-called classification societies (Walters and Bailey 2013, 98-99). Even before that, however, nation-states were already taking timid steps to regulate life at sea. In Danish history, state promulgated maritime law can be traced all the way back to year 1651, when Frederik the Second introduced the First Maritime Law, which sat rules for the relationship between masters and ship owners (Danish Maritime Authority 2018)[13]. In the case of Britain, the state's entrance into the business of regulating the maritime industry occurred officially in 1850, through the promulgation of the first Merchant Shipping Act "in response to unprecedented numbers of losses of ships and sailors" (Walters and Bailey, 2013, 100).

The fast development of world trade in the XX century made the regulation of shipping at the international level necessary. What begun as bilateral agreements between shipping nations led, after the tragedy of the Titanic in 1912, to the Safety of Life at Sea (SOLAS) Convention; the first and still "most important of all international treaties concerning the safety of merchant ships"[14]. The 1974 version of the Convention, which has since then received several amendments, establishes "minimum standards for the construction, equipment and operation of ships, compatible with their safety"[15], and leaves to the so-called Flag States the responsibility of ensuring compliance. SOLAS is usually depicted as the first step towards the creation of the IMO, which was established through a convention in 1948 (originally under the name of International Maritime Consultative Organization, IMCO), and entered into force in 1958, as a part of the United Nations. Besides the IMO, another international actor that plays a crucial role in regulating the maritime industry is the International Labor Organization (ILO), which focuses mainly on the safety and wellbeing of seafarers (Danish Shipping 2019). Due to the scope of this report, however, a focus on the role of the IMO is more relevant.

In spite of the IMO's weight in the maritime regulatory landscape, the clout of "flag states", which are the states wherein ships are registered, should not be ignored. States, and especially those with more leverage in the industry, not only are key players in shaping international conventions within the IMO, but also have a crucial role in

[13] Retrieved in 2 November 2018 from Danish Maritime Authority website. https://www.dma.dk/OmOs/VoresHistorie/NedslagSoefartshistorie/Sider/default.aspx

[14] Retrieved in 29 October 2019 from the IMO website. http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

[15] Ibid.

implementing and enforcing them, thus bringing into the picture an element of political realism. As it is the case with all international conventions, they have to be incorporated into national legislation, and it is the state that is responsible for implementation and enforcement. Thus, it is at this stage of the regulatory process that concerns regarding the achievement of a level playing field may emerge.

As known, the shipping industry struggles to find solutions to the problem of so-called "flags of convenience", "open registers" and the practice of "flagging out", which started in the 1980s due to the economic crisis that affected maritime shipping. We will not speak much about these issues, as they have been described at length by several scholars (see, for instance, DeSombre 2006). For the purposes of this report, it remains sufficient to mention that the relative "mobility" that flagging out has given to ship owners, in terms of allowing them to choose which regulatory regime their vessel will belong to, has represented challenges in the sense of providing a level playing field among states, and avoiding a "race to the bottom" (Almklov and Lamvik 2018, 176).

As a counterpoint, port state authorities have been granted the power to "board ships that enter their ports and inspect them for compliance with various international conventions" (Walters and Bailey 2013, 117), even when the state to which the flag is registered is not a signatory. This is known as the "no more favourable movement". Another important development in this direction are the so-called Memorandums of Understanding (MOUs), created to coordinate enforcement strategies among states[16].

The widespread idea that flags of convenience create regulatory and market distortions that may produce harmful consequences for the environment and for vessel safety has, however, been disputed. The study by Winchester and Alderton (2002), for instance, makes the case that registries that are too lax with regards to international regulation cease to be attractive in the long term, as they tend to be disproportionally targeted by inspection regimes. In brief, most "flag states today enforce a minimum of regulation and regimes of inspection to keep the ship in compliance with international standards" (Almklov & Lamvik 2018, 177, see also DeSombre 2006).

The meaning of the word regulation is rather contested, and may refer to a spectrum that covers both traditional "command-and-control" or deterrence-oriented legal approaches, which are centered on the state, and broader ideas of employing authority (stemming from sources as diverse as the law, market, social norms and even technology) to shape behavior (Brownsword et al. 2017, 6, se also Black 2001). Still, when we think of environmental protection, health and safety, traditional ideas of state-centered regulation are predominant. More specifically, there is "common agreement in Western societies that a legislative framework is needed to guide industrial behavior and to guarantee rights for workers, as well as for the environment" (Aalders and Wilthagen 1997, 42), since market mechanisms are insufficient. Despite this relative consensus on the greater effectiveness of deterrence-oriented legal approaches in the fields of health and safety and environmental protection, "less than traditional" formats of regulation have also been tested and approved.

Historically, alternatives to command-and-control were developed in all policy fields in the Western world in association with a wider criticism of the interventionist state and its social and economic costs. As Zuboff (2019) recounts, the stagnation and inflation that engulfed the postwar West formed the perfect environment for the neoliberal discourse of rolling back the state.

The free market creed originated in Europe as a sweeping defense against the threat of totalitarian and communist collectivist ideologies. It aimed to revive acceptance of a self-regulating market as a natural force of such complexity and perfection that it demanded radical freedom from all forms of state oversight (Zuboff 2019, 38).

It was also in this context that the theory of "shareholder capitalism" emerged. Its authors, inspired by free market proponents such as Friedman and Hayek, identified a gap between the interests and preferences of managers (agents) and the interests and preferences of shareholders (principal). Such gap, although rational from the point of view of managers, was problematic because it lowered the value of the firm and harmed the wealth of shareholders. The solution was then to "assert the market's signal of value, the share price, as the basis for a new incentive

[16] [16] A Memorandum of Understanding (MOU) is an administrative agreement between authorities. In the shipping industry the first MOU was the Paris Memorandum of Understanding on Port State Control. It was crafted in the wake of a major oil spil in the coast of France in 1978, which led to demands for stricter regulation. It was signed in January 1982 by fourtneen European countries and entered in operation in July 1982. It has been amended several times since then, and now counts with 27 signatories. Other MOUs have been created since then. Retrieved from the Paris MOU website in October 30, 2019. (https://www.parismou.org/)

structure intended to finally and decisively align managerial behavior with owners' interests" (Zuboff 2019, 39).

In spite of the influence of shareholder theory, counterpoints to the idea that businesses should merely aim at increasing the wealth of their owners did not take long to appear. The theory of stakeholder capitalism, for instance, departed from the principle that the organization "sits in a wider social context" and therefore needs to heed moral values and consider the interests of all of its stakeholders, even if "out of enlightened self-interest" (Aalders and Wilthagen 1997, 434). The perception, which lies at the heart of the concept of corporate social responsibility, that corporations should have "clearly articulated and communicated policies and practices (that) reflect business responsibility for some of the wider societal good" (Matten and Moon 2008, 405) became widely accepted, despite variations in configuration. In this context "doing justice in the workplace for employees, manufacturing safe products for consumers, caring for the environment, enhancing (rather than maximizing) shareholder value, and so on" became part of the agenda (Gunningham and Rees 1997, 375).

Interestingly, stakeholder capitalism, or the principle that firms are also accountable to society at large, is not necessarily associated with a dull defense of pure regulation and command and control frameworks, being in tune with different self-regulatory and co-regulatory models, including the idea of the "social responsibility" of the firm and "enterprise liability". As a sensible solution to regulatory overload, self-regulation may be seen as a "middle way between laissez-faire capitalism and state-centered regulation", which might be efficient in "bring(ing) the behavior of industry members within a normative ordering responsive to broader social values" (Gunningham and Rees 1997, 364). Moreover, its goal is to ensure that "firms or their associations, in their undertaking of business activities, ensure that unacceptable consequences to the environment, the workforce or consumers and clients, are avoided" (Gunningham and Rees 1997, 365).

The OECD has similarly defined industry self-regulation (ISR) as an efficient and less costly mechanism for "addressing consumer issues, particularly when business codes of conduct and standards are involved" (OECD 1997,5). In one of its reports on the topic, it describes ISR as the result of agreements between groups of firms in a particular industry or entire industry sector to act in determined ways. These groups "can be wholly responsible for developing the self-regulatory instruments, monitoring compliance and ensuring enforcement, or they can work with government entities and other stakeholders in these areas, in a co-regulatory capacity" (OECD 1997, 11).

As suggested above, "there is no clear dichotomy between self-regulation, on the one hand, and government regulation, on the other", especially because pure forms of private regulation (wherein both rule making and enforcement are done by the firm or industry) rarely exist (Gunningham and Rees 1997, 365). Conversely, governments are important agents in the wide range of "configurations" that characterize their partnerships with businesses in promoting acts that are socially responsible (Gond et al. 2011).Thus it is more productive "to think in terms of typologies of social control, ranging from detailed government command and control regulation to "pure" self-regulation, with different points of the continuum encapsulating various kinds of co-regulation" (Gunningham and Rees 1997, 366). In the case of corporate social responsibility, for instance, configurations may vary between "self-government (voluntary and non-enforceable) or as an alternative form of government (substitute for government), but also as self-reegulation which is facilitated by government, coordinated in partnerships with government, and mandated (…) by government" (Gond et al. 2011, 642).

As previously mentioned, the idea that self-regulation, understood as delegation of government authority to industrial associations and firms, can become an alternative to the centralization of regulatory authority in the state, has been discussed and tested in the fields of occupational safety and health and the environment. Aalders and Wilthagen (1997), whose study focuses on land-based self-regulation in these fields, provide an interesting comparison between them. They claim, for instance, that it is more easy to identify "interests, objectives, and structure of the actors" in the field of occupational safety and health than in the environmental area. This is the case because individuals have difficulty understanding their role as polluters and thus assuming responsibility. On the other hand, both employers and employees usually see themselves as responsible for safety and health. Second, the fact that pollution and the environment often have "transboundary consequences", turn them into very particular and less visible political questions, to the contrast of safety issues, which are rather well circumscribed (Aalders and Wilthagen 1997, 418). Somewhat paradoxically, however, the authors themselves cite different studies that draw attention to the fact that effective "self-regulation" within safety and health has

clear limits. For one thing, in order to work properly, it requires a high level of commitment, knowledge and motivation on the part of employees and, especially the commitment of senior executives and line managers. In other words effective self-regulation within safety requires employees to be active in identifying hazards, monitoring and implementing controls".More importantly, "without it being externally forced on them, people will often not take matters of safety and health seriously until they come into contact with severe injury or death" (Aalders and Wilthagen 1997, 421).

In the same special number of the journal Policy and Law that Gunningham and Rees presented their comprehensive assessment of self-regulation, Furger (1997) conveys his detailed study of self-governance systems within the maritime industry. He makes the claim that government regulation is not the only source of accountability, and that private institutions or "intermediary organizations", which do not necessarily follow jurisdictional lines, such as trade associations, protection and indemnity clubs, marine underwriters, classification societies and trade unions, may contribute as much as traditional regulators to the goals of safety and environmental protection within the global maritime industry. As an example, he cites Intertanko, the International Association of Independent tanker owners. This association offers a series of services to its members, but only upon the condition that they comply to strict requirements concerning safety and security (Furger 1997, 454).

Another example of self-regulation, this time pointed by different authors, is the Norwegian petroleum industry. This national industry is a successful example of self-regulation as a tool to countering the so-called "race to the bottom", which refers to a competition on who offers the lowest requirements. According to Almklov and Lamvik (2018, 181), there are incentives for petroleum companies "to go beyond minimal demands" or standards required by law. This is the case because "accidents and nonconformities in all parts of the value chain will be closely associated with the company operating the petroleum production licence" (Almklov and Lamvik 2018, 181). In other words, reputation and public image come into play, even when we are speaking of an industry that does not deal directly with consumers.

Finally, one example that is often cited in the broader literature on self-regulation within safety is that of the nuclear energy industry in the United States (Barnkenbus 1983, Ellis Jr. 2015). In this case, scholars refer to the Institute of Nuclear Power Operations (INPO), an industry association created in the wake of the 1979 Three Mile Island nuclear accident by the nuclear utility industry itself. The main roles of INPO are: the gathering, evaluating and sharing of information between all plants, on-site periodic evaluation and review with utility executives of performance, training of employees, setting standards and guidelines, job evaluation criteria, and examination of utility emergency preparedness plans (Barkenbus 1983, 584).

Although nuclear power plants are under no obligation to join INPO, it is widely acknowledged that the American Nuclear Regulatory Commission would never approve an unaffiliated plant. INPO and the National Regulatory Commission work together and depend on one another, to the extent that the latter deals with designing regulation, while the former focuses on the "operation side of things, the safety", thus producing a co-regulatory framework of governance (Ellis Jr. 2015). Moreover, INPO focuses on promoting a culture of safety, and building common standards and expectations for a safety culture, and focuses mainly on the involvement of top management (Ellis Jr. 2015). Also important is the fact that INPO's grading of the level of safety of a power plant translates directly into insurance premiums.

Going back to shipping, in spite of Furger's (1997) innovative attempt to reveal self-governance mechanisms within the shipping industry, his study gives little attention to one of the main parameters for safety and environmental protection within the shipping industry, namely, the International Safety Management (ISM) Code, which is also where cyber risk management is included. The ISM code has the purpose of providing an "international standard for the safe management and operation of ships and for pollution prevention"[17]. Its origins refer back to the late 1980s, when a series of maritime accidents caused by cost cutting took place and action at the international level was deemed necessary. Also importantly, such accidents were assigned to "errors on the part of management"[18]. The code thus establishes "safety-management objectives and requires safety management system (SMS) to be established by the "company", which is defined as the owner or any other organization or person (…) who has assumed responsibility for operating the ship"[19]. The ISM code became a part of the SOLAS convention[20] in 1994, which means that its application is

[17] Retrived from the IMO website in October 29th 2019. http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx
[18] Ibid.
[19] Ibid.
[20] Retrived from the IMO website in 30 March 2019. http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/Int

mandatory by signatory states. It progressed slowly from including only ro-ro passenger ferries to covering all types of merchant vessels over 500 gross tonnage by 2002 (Danish Shipping 2019).

The ISM code should not be seen as "an isolated provision", but rather as part of a "wider development of regulated self-regulation of health and safety management" (Walters and Bailey 2013, 130), which denotes a combination of government and private/voluntary initiatives. By the 1960s and 1970s, "command and control" approaches to health and safety had started to show signs of exhaustion. Side by side with this, there was a movement in the direction of adopting voluntary approaches to organizational health and safety management, partly encouraged by the development of quality standards and the Total Quality Management movement. These "land-based" experiences had a profound effect in "the development of systematic approaches to health and safety management at sea", including the development of the ISM code (Walters and Bailey 2013, 134).

The code, similarly to its land-based counterparts, puts considerable emphasis on the "human aspect" or human element of accidents, rather than on technological or equipment failure. Consequently, the improvement of management systems, and the introduction of a safety awareness culture are seen as the key to more safety. The ISM code, which is concerned both with the environment and safety, is based on six functional requirements: (1) a safety and environmental-protection policy, (2) procedures regarding the safe operation of ships and environmental protection in tune with international and national legislation, (3) clearly defined levels of authority and lines of communication between and among shore and shipboard personnel, (4) clear procedures for reporting accidents and non-conformities, (5) emergency response procedures and (6) internal audit and management review procedures (Walters and Bailey 2013, 137). Within this system of responsibility attribution, the ship master carries the largest amount of responsibility for ensuring the application of the code (Danish Shipping 2019).

It is also important to understand how the code is implemented, as outlined in its part B. The code requires that, in order to operate, a company has to be issued a "Document of Compliance" (DOC) or an Interim DOC. These are valid for 5 years and are specific to each ship. Ships must also have a Safety Management Certificate, which assures that companies are operating the ship in accordance to the "approved safety-management system" (Walter and Bailey 2003, 40). Verification of DOCs and SMCs with regards to their validity may be done either by national maritime authorities or delegated to classification societies, consultants or other flag state administrations.

Now that we have a more or less clear picture of general issues concerning cybersecurity and its regulation, as well as general aspects of regulation in the shipping industry, we can move into the last section that precedes the exploration of the Danish case, namely, the section which discusses the role of technology as a regulator.

ernational-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

THE ROLE OF TECHNOLOGY AS A REGULATOR

As mentioned above, there is a fair amount of consensus in the literature about the fact that there "are no direct technical solutions to addressing systematic risk", since it is also "a natural side effect of complex systems" (Friedman 2011, 1). Still, technology, design, and artefacts in general can perform the role of "regulators" by leading (or even coercing) humans towards certain (desirable) course of action and behaviors – egg. speedbumps physically preventing a vehicle from exceeding speed limits. Technology can also be its own "regulator" or be "secure by design", such as in the case of software that automatically updates.

The term "techno-regulation", created at the interface of the disciplines of IT law, science and technology studies and philosophy, refers basically to the use of technologies or artefacts to enforce socially desirable behavior (Brownsword et al. 2017, Yeung 2017), and has a strong basis on Lessig's (1999) principle that "code is law", as well as on Winner's (1986) idea that technology has inherent politics. The main point of technoregulation, however, is to push or even coerce humans into taking desirable/law-abiding/moral courses of action. Thus it is more closely related with "nudging" than with security by design solutions. In the case hereby discussed, it could amount, for instance, to promoting positive behavior (i.e. an email from management thanking employees who heeded information security policies) and giving feedback, investing on visual communication, and behavioral changes through training (Hulgaard 2018). As described by Yeung (2017,3), "one of the greatest attractions of utilizing technology to tackle social problems lies in the potential to achieve its behavioral objectives with 100 per cent effectiveness and in circumstances where design is self-enforcing so that no human intermediation is required to secure compliance with desired standards". This means, among other things, the recognition that humans are prone to error and that human behavior is unpredictable. In the case of cybersecurity, this becomes even more apparent, due to vulnerabilities that can result from "lapses in cyberdiscipline" (IMO 2017b), or from the reckless conducts of individuals, such as in the cases above described by Arduin (2018).

Artificial intelligence, for instance, while bringing its own challenges in terms of cybersecurity, may also enhance it in unprecedented ways, since "security techniques that range from phishing detection and surveillance systems to fundamental cryptographic algorithms are becoming increasingly powerful and intelligent with the help of AI" (Fang et al. 2018, 2). Still, important distinctions should be made between "security by design" types of solution (for example, systems that update or backup automatically, segmenting networks, or enforcing strong passwords), the use of technologies such as AI in the detection of cybersecurity threats, and something in the vein of "techno-regulation". The latter amounts to using technology to direct or even "nudge" human behavior, so that it is headed into the expected direction.

After having considered the elements of regulation, self-regulation and technoregulation in the literature, and provided a brief account of information security, it is now appropriate to move into the findings or analysis, which focuses on the exploration of the Danish case.

CYBERSECURITY IN THE DANISH SHIPPING INDUSTRY: AN EXPLORATORY STUDY

In the beginning of 2019, the Danish Maritime Authority released its Cyber and Information Security Strategy for the Maritime Sector, a three-year plan associated with the Danish Ministry of Finance's 2018-2021 Cyber and Information Security Strategy. In the latter, the maritime sector was considered as one out of six "critical sectors" deserving of a specific sectoral strategy in the field of information and cyber security. This policy focus on cybersecurity, more broadly, and on cybersecurity in shipping, in particular, is in tune with Denmark's pride in digitalization, and the importance of maritime shipping for the national economy[21]. And yet, it is worth noticing that the national governance framework is closely connected with a wider international co-regulatory structure. This became evident throughout an analysis of the primary data collected for this project, which is here organized into 4 interconnected codes or categories, namely (1) "regulation, self-regulation and accountability", (2) "safety, security and the ISM code", (3) "information sharing, awareness and brand sensitivity" and (4) "security by design, nudging and the human factor". As mentioned in the methodology section, these codes were developed with the assistance of theories and categories in the literature, but adapted on the basis of the primary data itself. These categories are hopefully able to provide us with a clearer picture of the governance framework for cybersecurity in the Danish shipping industry.

REGULATION, SELF-REGULATION AND ACCOUNTABILITY

One of the points that have repeatedly come up in the interviews and other sources consulted for this research refers to the importance and effectiveness of regulation within the shipping industry. In the particular case of cybersecurity in vessels, this happens not the least because regulation sets up "minimum requirements", or a "common ground", amidst a sea of different levels of "technological readiness" on the part of shipowners (Christiansen 2018). Since organizations within the shipping industry "are very diverse" in terms of their reliance on IT and investment on digitalization, regulation becomes even more important in the sense of ensuring a minimum degree of safety of systems. Conversely, regulation could also be seen as a "driver of innovation", to the extent that it may push towards "better technical solutions to problems such as cyberthreats" (Christiansen 2018).

The ubiquity of regulation in maritime shipping is pretty straightforward. After all, "if a ship does not follow standards it won't be classified, and thus it will be detained…. So there is absolutely not a chance" (to stray from regulation) (Glamsø 2018). Here, although classification societies may have an indirect role in regulation, at the end it is states that are the main points of accountability. This happens, among other things, because the regulatory structure is based on international conventions that are implemented by states, and which aim at offering a level playing field (Glamsø 2018).

Although regulation is a powerful tool in promoting a level playing field, it could also work in the opposite direction, so that "some players are favored at the expense of others" (Larsen 2019). Avoiding this imbalance is at the heart of what an organization such as BIMCO does, to the extent that it "tries to be that voice among the regulators that explains (…) the impacts of a given piece of legislation". That is, "how can you arrange a piece of legislation so that it works in the market, and is effective without creating an unlevel playing field" (Larsen 2019).

A good illustration here is that of short deadlines for implementing new rules for technical installations on board. Short deadlines might do harm to a shipowner with a large fleet of older vessels, whereas shipowners who tend to build new vessels can more easily adapt their newbuildings to the rules. Therefore, reasonable deadlines for implementation, which offer "time to adapt" or allows for "grandfathering" of existing vessels, are crucial (Larsen 2019).

As mentioned before, one of the most important tools for achieving a level playing field is international regulation

[21] There are many evidences of the seriousness with which digitalization is taken up in the Danish shipping industry. In 2018, for instance, the then Prime Minister Lars Løkke Rasmussen

crafted at the IMO, as it sets the same rules for all signatory parties. Still, jurisdictions with sufficient political and economic clout have been able to enforce their own rules. The examples of the United States after the 9/11 attacks is telling (Jensen 2018). Pressed by this paradigm changer event, the country was able to enforce regulation demanding that shipping lines list the content of containers onboard ships with at least 24 hours prior to leaving port towards that country. The weight of this political actor shouldn't be ignored here: "because the US is as big as it is, and as important as it is, the rule went into effect and everybody complied" (Jensen 2018).
Although special or particular national rules might be important in some cases (egg. for protecting a particular maritime ecosystem), these should not be abused, as it might be quite confusing for ship owners.

Compare to driving on the road….If every time you went to a new country you had different traffic signs and new rules (…) it would be really difficult to be a truck driver. (Therefore,) it makes sense to try to keep the same rules, (and then) you can (even) set a high standard, as long as it is the same (for all) (Larsen 2019).

Moving now into the field of self-regulation, it is interesting to note that in its 2011 report on cyber risks within the maritime sector, ENISA (2011, 14) makes the claim that "self-regulatory and co-regulatory organizational models around maritime cyber security" are not only "virtually non-existent" within the EU, but also "inadequate in this particular case". Such claim was echoed by the informants who, while advocating for the need for regulation have, conversely, shown at least some degree of skepticism towards the idea of self-regulation. On the other hand, they did acknowledge the importance and effectiveness of initiatives such as BIMCO et al.'s guidelines, even if these were by no means associated with mandatory compliance, that is, "external auditing of vetting (of) the individual company's and ship's approach to cyber risk management" (BIMCO et al. 2018, 4). Apparently, the skepticism regarding self-regulation is associated with the perception that, in the absence of enforcement and punishment for violators, most organizations will not voluntarily comply with requirements – unless, of course, they can be translated into savings. For Jensen (2018) the matter is "at heart" simple: "if you save money by doing something, it will self-regulate". If not, "if it is mandated by law, and the law is enforced (both things have to occur!), then it gets done. Otherwise it doesn't".
The environmental area is a good example. In it, "self-regulation would not be effective, since "the impacts of one's (wrongful) actions are not immediately felt by the person who is performing those actions" (Larsen 2019).

(But Cybersecurity) is different, because if you mess up with your cybersecurity you put your own company at risk (…) So here, I think, regulation becomes more a question of setting the frame (…) Perhaps, if its very technical, defining some standards (would be enough). But then the exact level to which you want to protect your business could perhaps be left to the individual company (Larsen 2019).

The same informant, however, recognizes immediately that further distinctions concerning externalities might be relevant when claiming that "in certain sectors or for certain providers of essential services", stricter regulation and enforcement might be relevant due to the "wider implications" of cyber threats, in terms of affecting society as a whole. Once again, we are reminded of the connection between cybersecurity and the safety of vessels, which is the topic discussed below.

SAFETY, SECURITY, AND THE ISM CODE

As mentioned before, all of the informants agree with the principle that regulation of maritime shipping is necessary. Moreover, they acknowledge that cybersecurity, in particular, should be regulated at the international level. At the IMO, maritime cyber risks are defined as "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" (IMO 2019).[22] Their regulatory and governance effort in this field materializes into a set of guidelines and one resolution. The latter , resolution MSC 429(98), Maritime Cyber Risk Management in Safety Management Systems, which was adopted by the Maritime Safety Committee in June 2017: (a) affirms that "safety management systems" should take into account cyber risks management in accordance with the objectives of the ISM code, (b) encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems "no

[22] http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx

later than the first annual verification of the company's document of compliance after 1 January 2021", (c) acknowledges that certain precautions are necessary to preserve confidentiality of cyber risk management, and, (d) requests member states to bring the resolution to the attention of stakeholders (IMO 2017a).

This resolution had as background the Guidelines on Cyber Risk Management, approved earlier in the same year by the Facilitation Committee and the Maritime Safety Committee. These guidelines intended to "provide high-level recommendations on cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities" (IMO, 2017b).

It is important to understand some of the particularities concerning the above mentioned resolution, in particular regarding ambiguities concerning the management of cyber risks under the ISM or the ISPS codes. According to a document submitted by the United States, ICS and BIMCO to IMO's Maritime Safety Committee in March 2019, parts of resolution MSC 429(98) were not so clear, and needed to be addressed. More specifically, the co-sponsors were concerned that the resolution could be interpreted as prioritizing provisions of the International Ship and Port Facility Security (ISPS) Code over those of the ISM code for cyber risk management. They also claimed that too much focus was being given to "counter external, malicious threats rather than providing a more holistic cyber risk management approach following the principles established in the ISM Code" (United States et. al. 2019, 2).

Apparently, it makes sense to manage cybersecurity under the ISM (rather than ISPS) code due to its greater level of flexibility, which is more in tune with the rapidly changing landscape of cyber threats and technological development (Larsen 2019). More specifically, if cybersecurity goes under the ISPS, it means that it will be associated with the ship security plan, which is less flexible to changes, because each update to the plan has to be approved by authorities. This would also represent a larger cost for shipowners. Particularly in the case of shipowners with scarce resources, this could lead to postponements in updating important systems, thus making regulation suddenly "defeat its own purpose" (Larsen 2019)[23].

Glamsø (2019) agrees, as it would represent "a huge cost and a bureaucratic hurdle" if cybersecurity were to be included in the ship security plan (under the ISPS code), rather than in the safety management plan (under the ISM code).The ship security plan is confidential, and cannot be verified by the port authority, while the safety management plan can. Inclusion into the ISM code would, in turn, allow for "greater responsiveness to emerging cyber risks identified by a company", considering also that it would provide "a comprehensive framework for addressing cyber risks" (United States et al. 2019, 3).

The view that cybersecurity should be included into the ISM code owes partly to an understanding of the nuances between safety and security[24]. For Larsen (2019), the term security is more clearly associated with "the result of a deliberate act by someone who wants to hurt you and/or create a benefit for themselves at your expense". That is why he and BIMCO prefer to talk about cyber risks management rather than cyber security. When it comes to cyber incidents that affect the operation of ships, maliciousness is not always the case (United States et al. 2019, 1), and therefore, the association with the ISPS code might be not only inefficient, but also semantically wrong. Conversely, it is not always the case that cyberattacks have safety implications for ships. As an example, one could mention hackers accessing a ship's administrative network to get access to commercially sensitive information about the cargo (Larsen 2019, Jensen 2018). This would characterize industrial espionage and would be considered an information security crime. Still, it would not imply a safety threat for the ship, and thus would not be covered under the ISM code (which does not address commercial issues).

On the other hand, in the case of a vessel, a "security" issue might rapidly become an issue of safety for the vessel and its crew. For instance, one could think of the hypothetical case of someone hacking into the ship's engine control system from the outside and switching off the main engine, thus leading to a safety threat (Larsen 2019). Similarly, a virus could stop the engine of a ship, and thus become a safety issue (Glamsø 2019), thus touching upon the problem of externalities.

[23] The ISPS Code is focused on responding to external threats, malicious actions and physical security, and in this respect provides an incomplete framework for effective cyber risk management as outlined in paragraph 2.1.4 of MSC-FAL.1/Circ.3. Moreover, changes to the approved ship security plan require approval by the Administration. This reduces the responsiveness of companies to newly identified cyber risks, and introduces a potentially significant and frequent administrative burden for Administrations

[24] As noted by Glamsø (2019) in the particular case of Denmark, there is potential for confusion between the terms safety and security, as the same word (sikkerhed) is usually used in reference to both.

Suppose your computer at the university gets infected…. Then the problem is (basically) for you. But if a hospital gets infected with a virus, it can have greater consequences for society, and regulation is thus necessary (Glamsø 2019).

The analogy with cybersecurity in shipping makes sense, specially given that the consequences are not only commercial, but can also affect safety. Then the ISM code is there because "it assigns responsibility to shipping companies for cyber risk management". If it weren't for this, "you could always blame someone else, like the captain" (Glamsø 2019).
BIMCO et al. (2018) also make this connection between safety and security, while at the same time proposing a distinction between "cyber security" and "cyber safety". As mentioned in their guidelines, both cyber security and cyber safety should be heeded due to their safety implications: that is, due to "their potential effect on personnel, the ship, environment, company and cargo" (BIMCO et al. 2018, 3). Still, while cyber security "is concerned with the protection of IT, OT, information and data from unauthorized access, manipulation and disruption", cyber safety covers "the risks from the loss of availability or integrity of safety critical data and OT" (BIMCO et al. 2018, 3). In other words, cybersecurity is related with maliciousness and with the causes of disruption, while cyber safety, which is the principal focus, deals with the consequences of such maliciousness for the integrity of the vessel, its equipment, crew and cargo[25].

INFORMATION SHARING, AWARENESS AND BRAND SENSITIVITY

As discussed in several policy documents and scholarly publications, one of the most effective ways to respond to, and prevent, cyber incidents is information sharing. The findings have confirmed this, but also led us to understand some of the challenges associated with this practice – challenges which are either related with the nature of cybersecurity, particularities of the industry or both.
In general, the expectation behind information sharing is to "help other members (of the industry) by means of awareness" and "learn through one another's examples" (Christiansen 2018). Awareness is indeed a crucial aspect when it comes to preventing attacks, especially within an industry that "still doesn't see itself as a main target of cyber attacks", but mostly as collateral damage (Christiansen 2018).
The picture, however, might be changing for the better. A 2017 survey conducted with CEOs from Danish shipping companies has shown an increase (as compared to the previous year) in the level of concern with cybercrime, something that was translated into practical actions, such as more robust IT security budgets (Danish Shipping 2018). This was likely a reaction to the Mærsk attack, which occurred in the summer of the same year. Still, one should not ignore that "there are signs of a gradual change of mentality" (Christiansen 2018). Industry members thus seem to have internalized that there is a "high threat level posed by cyber criminals in the shipping industry", even though it is "primarily directed at commercial operations and generally do not represent a direct threat to physical security interests and not particularly at physical security in the maritime sector" (Danish Defense Intelligence 2017Centre for Cyber Security 2017). Danish Shipping also backs this statement, when mentioning that the immediate risk is related to the security of data (Danish Shipping 2019). Still, there is the recognition that companies "operating in conflict areas", may become "collateral damage in connection with destructive cyber attacks" (Danish Defense Intelligence Service 2017, 13).Something that may also contribute to a higher level of awareness among Danish ship owners with regards to cybersecurity is the fact that the maritime sector has been considered as one of the priority areas in the field of information security. As previously mentioned, in the Danish Ministry of Finance's Cyber and Information Security Strategy, published in 2018, six critical sectors were announced as deserving of specific and carefully tailored information security strategies, namely, energy, healthcare, transport, telecommunication, the financial sector and the maritime sector. The latter, according to the strategy, covers "security related to navigation in Danish Waters as well as security of ships registered under the Danish flag, together with their crew". Moreover, "cyber security for ships includes services such as traffic monitoring, warnings and navigation information (AIS, NAVTEX), systems used by ships and software for operation of the ship, including propulsion and navigation" (Danish Ministry of Finance 2018, 37)[26].

[25] Cyber safety incidents, according to BIMCO's guidelines, could arise as the result of: "a cyber security incident, which affects the availability and integrity of OT, for example corruption of chart data held in an Electronic Chart Display and Information System (ECDIS), a failure occurring during software maintance and patching, loss of or manipulation of external sensor data, critical for the operation of a ship – this includes but is not lmited to Global Navigation Satellite Systems (GNSS)".

[26] It is also important to mention that the raising of awareness has been central in the 2015-2016 cyber and information security strategy in Denmark.

The level of awareness regarding risks has also an important correlation with information sharing. When it comes to sharing information regarding attacks, two obstacles can be highlighted. The first refers to the fact that many attacks go undetected or take too long to be detected, while the second refers to the unwillingness to share information on them due to geopolitical concerns, fear of alerting the attacker and/or brand sensitivity. As to the first category (i.e. lack of knowledge about an attack), it is worth noting that it can take "on average 140 days between time of infection of a victim's network and discovery of a cyberattack", and that years could go by before an intrusion is detected (BIMCO et al. 2018, 11). Munro (2018), referring to the extreme example of the hacking of a ship, argues that this does not happen like usually shown in films. In other words, these attacks are "rarely visual" and thus "hard to detect", thus challenging the usual claim that manual control over a vessel would easily counter it.

Regarding the second challenge listed above (i.e. unwillingness to share information), even more obstacles are encountered, which are translated into the recognition by the IMO (2017b) of the fact that "precautions are necessary to preserve confidentiality of cyber risk management". In 2014, Cyberkeel (now part of Improsec) published a whitepaper wherein it proposed, among other things, the creation of a forum or alliance within the shipping industry: a "trusted environment wherein companies can share specific technical details of ongoing cyber attacks to allow similar companies to easily scan, detect and deflect identical attacks" (Cyberkeel 2014, 25). The proposal never came into fruition due to particularities of the shipping industry that cannot be ignored. According to Jensen (2018), for an alliance of such nature to work there "has to be trust", and this may be a challenge in a "truly global industry". When one considers, for instance, that some carriers are "state owned" and that "threat actors" may be government themselves (see, for instance, von Seelen 2018 and BIMCO et al. 2018), the geopolitical obstacles to this kind of alliance becomes palpable. Here, it is important to recall that the NonPetya attack that paralyzed Maersk for 10 full days in 2017 was not aimed at the company itself but began rather as an assault of one nation (Russia) on another (Ukraine) (Greenberg 2018, 6). It is in this context that the intermediation of government authorities might be necessary. In Denmark, for instance, the recognition that "awareness of threats, identification of vulnerabilities and assessment of risks" are crucial parts of a Cyber and Information Security strategy has led to the establishment of a National Cyber Situation Center within the so-called Centre for Cyber Security[27] (Danish Ministry of Finance 2018, 20-21). This center is responsible for receiving and processing information on cyber incidents that authorities and certain types of businesses are required to report. As an additional tool for facilitating the gathering of information, the government created a single digital solution for reporting security incidents (Danish Ministry of Finance 2018, 24). In connection with the broader national strategy and the specific sectoral strategy, a Danish Maritime Cybersecurity Unit has also been created "to provide advice and (…) serve as a communication hub with respect to cyber and information security for the entire maritime sector" (Danish Maritime Authority 2019, 5).

The need to establish a safe channel to report breaches of security is also part of the implementation of the EU's NIS Directive, of May 2018, which takes us into the field of regional regulation. From this directive, it follows that "operators of essential maritime services in the maritime sector must notify the Danish Maritime Authority (the Danish Maritime Security Unit) and the Centre for Cyber Security of incidents having had a significant impact on the continuity of the maritime services they provide" (Danish Maritime Authority 2019, 5). Besides this, and as a part of compliance with regulation, Danish ship owners and ships "using network and information systems" are required to "incorporate cyber security in their risk management measures" and have to "notify the Danish Maritime Authority and the CFCS of any incidents" that are covered under the Order laid down by the Danish Maritime Authority (Danish Maritime Authority 2019, 5). Finally, it is important to mention that the Danish Maritime Authority will work "as an exchange point between the maritime sector players and the CFSC" (Center for cybersecurity) (Danish Maritime Authority 2019, 8). This intermediation could work in assuaging concerns regarding the exchange of sensitive information among companies who have other countries as shareholders.

Moving beyond the field of geopolitical concerns, information sharing may also be hindered by the legitimate concern that it will alert the attacker, who might then get a competitive advantage in terms of modifying/improving his/her strategies and attacking again. Finally, also in the category of obstacles to information sharing one finds the issue of brand sensitivity and impact on one's reputation.

[27] The Centre for Cyber Security is a national ICT security authority, "responsible for preventive national advisory and information activities associated with cyber security in both the public and private sectors" (Danish Ministry of Finance 2018, 22).

That is, sharing information on an attack may send a signal "that you are not in control of your business" (Larsen 2019). Mærsk, however, has been "very open" about its Notpetya attack (Larsen, 2019), among other things because the incident was of large proportions, and thus difficult to conceal, but also because the NonPetya was conducted by a state actor by means which fall outside the capabilities of commercial companies to defend against.
The lack of reporting has also proven a challenge in the case of maritime insurance. As Jensen (2018) mentions, in order to consider insurance for cyber incidents, insurance companies would ideally have access to the "statistics". However, due to the fact that few organizations report incidents, these statistics do not exist. ENISA's report confirms this concern, as it recommends that access to statistics on cyber security, derived from better information exchange would "help insurers to improve their actuarial models, reduce own risk" and thus offer "better contractual insurance conditions to the involved maritime stakeholders" (ENISA 2011, 21-22). A more active role by insurance companies in this field, the agency adds, would add economic incentives to heeding cybersecurity within the maritime sector.
The International Union of Maritime Insurance (IUMI) has recently crafted a position paper on the matter. According to IUMI, although "stand-alone ransomware insurance products are now available", insuring "consequential damages to hull, cargo and third-party liabilities from a cyber-attack on board a vessel or mobile offshore" is much more complicated and risky. This is the case, among other things, due to the "limited data (available) on the frequency, severity of loss or probability of physical damage" (IUMI 2019, 1) caused by cyberattacks.
The so-called "cyberexclusion clause" is, however, subject to several shortcomings. If, for instance, a ship sinks due to a cyberattack chances are that underwriters will never know the real cause, "and yet they may cover the accident, which in practical terms means that they are already covering cybersecurity issues" (Jensen 2018). In other words, the lack of information on the causes of an accident make the cyber exclusion cause inefficient in some instances.
BIMCO, however, as a first mover in the field, has recently drafted a standard Cyber Security Clause that "requires the parties to implement cyber security procedures and systems, to help reduce the risk of an incident and mitigate the consequences should a security breach occur" (BIMCO 2019). Getting coverage for cybersecurity incidents, however, also demands heeding the technological apparatus, and therefore the importance of moving into the next category, which concerns technology.

SECURITY BY DESIGN, NUDGING, AND THE HUMAN FACTOR

In a 2011 report ENISA (2011, 2, 11) wrote that due to high ICT complexity, it would be important to ensure "security by design" for all critical maritime ICT components. This claim is also reflected in the belief, specially on the part of senior management, that technology is the main solution for information security issues. Our informants, although aware of the importance of technological solutions, have painted a slightly different picture: one wherein more investment in cybersecurity suites does not automatically translates into more security. Jensen (2018) emphasizes this point by making use of two analogies:

It is as if you were running a music festival and said that the safety of everyone depended only on the guards manning the gates (…) It doesn't quite work like that!". Similarly, he adds, "it is useless to have a sophisticated alarm system at home if you forget to lock the door" (Jensen 2018).

Of course, procedures such as designing networks so that they can be physically segregated by the swift removal of a cable are important (von Seelen 2018). But these are simple, rather than technologically sophisticated procedures. Conversely, for most problems "there is no technical fix, but rather a human fix (Jensen 2018).
As an example of the importance of human behavior in assuring cybersecurity, one can cite the example of mundane but potentially dangerous practices, such as the posting on social media of information regarding a vessel's location, or of the fact that the manager is away at a business trip (Jensen 2018, Larsen 2019). Another example that is also related with human behavior, rather than with technology, is the use of weak passwords. Surprisingly, situations wherein the user name and the password are obvious, and connected to one another in obvious ways, are still pretty common (Munro 2018). Here, at least, the enforcement through technology of stronger passwords may assuage the problem.
It is based on this assumption that techniques such as "nudging" have been considered fruitful. In the case hereby discussed, nudging could amount, for instance, to promoting positive behavior (i.e. an email from management thanking employees who heeded information security policies) and giving feedback, investing on visual

communication, and behavioral changes through training (Hulgaard 2018). Moreover, management needs to understand that "increased levels of cyber security (will come) at the price of having to modify business processes in such a way that daily business operations might be impacted" (Cyberkeel 2011, 2).
Another problem related with information security and technology lies in the lack of control over vendors. As Jensen mentions (2018), many systems are basically sold on what he calls "IKEA mode", meaning that they cannot be altered.

Your load master systems, your navigation systems, all these different ones you buy from a third party, where not all these third party providers are so savvy into cybersecurity either (…) You can of course go to the vendor and say that this is not good enough. But the vendor would likely say, sorry, that is what we sell (Jensen 2018).

The problem might become even more complex if we think ahead, in terms of remote controlling of ships and even autonomous ships. Here, questions of security by design, accountability and responsibility, "also in terms of vendor responsibility", might become increasingly relevant (Glamsø 2019).
Understanding the importance of vendors in the chain of accountability BIMCO et al (2018) have also included in their guidelines a recommendation for companies to "define their own minimum set of requirements to manage supply chain or 3rd party risks" (BIMCO et al, 2018, 8). Already on phase 1, called the pre-assessment phase, the guidelines suggest that companies should identify main producers of critical shipboard IT and OT equipment and identify cyber-security points-of contact and a working relationship with each of them. The Danish Cyber and Information Security Strategy, while applying to a broader field, also highlights, under the category of "joint efforts", the importance of managing "suppliers of outsourced IT services" (Danish Ministry of Finance 2018, 17). At the Danish Maritime Authority's strategy, which follows from it, the need to control suppliers and outsourcing is described as an effort "to strengthen supply chain management". In other words, considering the increasing digitalization of vessels and complexity of systems, there is a significant degree of outsourcing, which increases in turn the importance of assuring "supplier's security level" and "quality performance" (Danish Maritime Authority 2019, 6).

Another important aspect concerning the relationship with vendors and cybersecurity refers to the increasing proximity between Operational Technologies (OT) and Information Technologies (IT). As the BIMCO et al. guidelines mention, "IT and OT systems software and maintenance can be outsourced to third-party service providers and the company, itself, may not possess a way of verifying the level of security supplied by these providers" (BIMCO et al. 2018, 17). To be sure, OT systems control the physical world (egg. hardware and software that control physical devices and processes) while IT systems deal with data. However, due to internet and technologies such as sensors and internet of things, both are getting much closer to one another (see Danish Ship Finance and Rainmaking 2018) and the difference is getting blurred. This blurring of boundaries, however, should also be reflected into different practices, such as a closer connection between IT departments and chief engineers responsible for purchasing OT systems (BIMCO et al. 2018).

DISCUSSION AND LIMITATIONS

We started this research effort with a couple of assumptions about the governance of cybersecurity in maritime shipping. More specifically, we assumed that although the shipping industry is known to be heavily regulated, self-regulation (or even no regulation at all) would be sufficient in the case of cybersecurity. In other words, given that it is on the self-interest of organizations to heed cyber hygiene, imagining a complex cybersecurity governance framework appeared to make little sense. At the early stages of the project, another assumption was that new technologies, particularly with the development of artificial intelligence, would play a crucial role in assuring cybersecurity with the least possible interference of humans. Throughout the process of collecting data for this research, however, we have come to dispute and/or refine some of these assumptions and arrive at new conceptions, which are listed below.

First, the maritime shipping industry is very careful in its selection of words and framing when it comes to the security of information systems. More specifically, it is meticulous in defining the specificities of the cyber threats which affects it, thus heeding to important categories suggested in the literature on cybersecurity, information systems security and cybercrime. If we use Friedman's (2011) three broad areas of cybersecurity, for instance, we may claim that most stakeholders within the shipping industry, as well as regulatory authorities, agree that industrial espionage and cybercrime are currently the main hazards to be confronted in the field of cyber and information security. Conversely, they assuage the magnitude of the risks within the field of national security – at least in times of peace. Within these two broad areas (espionage and cybercrime), the "machine", or digital technologies, function as mere tools in what Wall (2017) calls "crimes that use the machine". In other words, these are traditional crimes, that could have been conducted through different (non-digital) media, such as a phone, or even without the assistance of technologies. The only difference is that they have been given a "new", digital face, and possibly more efficiency. The category of "crimes against the machine" (Wall 2017, 180), as seen in the case of Mærsk, are also a possibility. However, this is usually considered an instance of "collateral damage", rather than a targeted attack.

Another related point is the association between cybersecurity and the intention of causing harm. Using the categories proposed by Arduin (2018), we have seen from the analyzed data that most information security incidents in the shipping industry occur either due to unintentional or to intentional but non-malicious actions on the part of employees, thus leaving out the category of intentional and malicious. However, if we consider that the victim in this case is always the shipping organization, employees within the organization (i.e. the human element) may either be the intentional perpetrators or criminals, which is rarely the case, or a mere instrument of the crime, in the same way as the technology. In other words, "crimes that use the machine", to use Wall's (2018) category, perpetrated by diverse types of cybercriminals, are also crimes that "use" humans (intentionally or not) as mediators, which blurs the distinction between these categories. This conclusion reinforces Arduin's (2018) comprehensive understanding of information systems as including humans, and corroborates what has been highlighted by several sources: namely, that humans are both the biggest obstacle as well as the main solution to cybersecurity. Moreover, probably due to this subtle understanding that most cyber incidents in the shipping industry are not intentional that the word cybersecurity in being used with parsimony and care, and other terms such as "maritime cyber risk management" and "cyber safety" are preferred.

At this point, we may approach issues of regulation and self-regulation. As noted by the informants, the potential problem of a "race to the bottom" or an "unleveled playing field" applies not only to issues such as environmental protection, but potentially also to cyber risk management, thus making regulation necessary. The reason for this regulatory penchant, however, has to do specifically with the fact that cyber risks are mainly associated with safety issues in shipping, to the extent that information technologies (IT) are currently connected with operational technologies (OT). As the literature has shown, and the sources interviewed corroborated, history has proven that safety records are negatively affected in the absence of regulation. Therefore, if cyber hygiene is positively

correlated to safety, it should as well be regulated. Moreover, there are both positive and negative externalities in cybersecurity, which the market alone cannot resolve, and this demands that regulators step in. What most informants do not discern, however, is that the governance framework we currently see in the industry is closer to a co-regulatory than a pure regulatory model in cybersecurity, or what Walters and Bailey (2013) would call a "regulated self-regulatory" model. This is the case because more traditional regulatory tools, such as inspections by port authorities, are combined with the use of guidelines, such as the ones produced by BIMCO et al. (2018). Moreover, the very inclusion of cyber risks within the ISM code gives a lot of leeway and flexibility for organizations, thus departing from traditional command-and-control options.

As seen in the literature, even in instances where negative externalities are clear, such as in the case of pollution and the nuclear industry, some form of regulated self-regulation is possible and effective. In other for this to work, however, employees and employers, and particularly managers, have to take up responsibility, and understand that their actions affect not only the organization's finances, but also its image (see Aalders and Wilthagen 1997, 421).

The connection between cybersecurity and vessel safety also opens up the path for an incursion into the field of corporate social responsibility or enterprise liability. The principle that organizations are accountable to society at large, which is supported by stakeholder theory, is easily shown in countless instances wherein the environment and workplace safety are at stake. Therefore, from the moment one connects cybersecurity to safety (a connection that is done through the material connection between IT and OT), one opens up the possibility of framing cybersecurity as an issue of corporate social responsibility.

To that extent, this report recommends that cyber hygiene be directly and more explicitly associated with the vessel's safety, as well as with social responsibility and accountability. Similarly to the way in which some organizations keep track of, and promote, the amount of days in a row without workplace accidents, shipping organizations could explore a similar strategy, wherein workers feel that, by taking care of the safety of information systems, they are actually benefitting the whole of the organization and also society as whole. For this connection to be made, however, it should be understood that:

- Not all cyber security incidents are intentional
- Information systems affect the safety of vessels
- Humans, rather than technologies alone, are the most important points of resistance

The proposed strategy is to some extent not so different from nudging, although the idea here is to use accountability and responsibility as an incentive for correct behavior. We should also observe that it makes sense to focus on the issue of cyber risks as being one of safety, rather than systems integrity, which is usually seen as highly technical and might be associated with low levels of self-efficacy on the part of employees.

Having said this, we do agree that regulation needs to remain in place, and that the governance model that the IMO has suggested for cyber risks (i.e. the ISM Code) is adequate, considering mainly that they take into account something that the data has shown, namely, that it is more a managerial and organizational, than a technical issue. We also believe that, at the national level, Denmark has promoted effective initiatives to govern cyber and information security in maritime shipping by acknowledging the particularities of this sector, the importance of establishing a dialogue with regulators at different tiers, and the importance of education and the human factor.

Now before we reach the conclusion of this work, it is important to acknowledge some of its limitations. First and foremost, we should recognize the limited amount of informants we accessed. Ideally, we would have interviewed informants from the Danish Maritime Authority, from other Danish governmental authorities, and possibly from IMO and ENISA, in order to increase the robustness of the findings through the consultation of national, regional and international regulatory authorities. Interviews with other industry stakeholders and even with ship operators would also have benefitted this research. Another path that we did not pursue, and which also constitutes a limitation, is a more thorough exploration of the current technologies used in the maritime shipping industry and how they affect cyber resilience. Finally, it is also important to highlight that the research was mostly exploratory, and does not consist of a comprehensive study of the Danish case – thus the choice of using "Danish maritime shipping industry" in the title, rather than the terms "case study" or "Danish case".

CONCLUSION AND SUGGESTIONS FOR FUTURE WORK

This report concludes a one-year project that investigates the nature and adequacy of the governance framework for cyber security in the maritime shipping, using the Danish shipping industry as a reference case. Besides different literatures, we have analyzed several reports and regulations, which were supplemented with data collected through interviews and participation in workshops.

We argue that the development of technology is connecting IT and OT to such extent that cybersecurity is intrinsically connected with safety in maritime shipping, thus making regulation necessary. This does not, however, invalidate self-regulatory initiatives on the part of industry associations, which are fundamental in providing parameters for best practices and for proposing additional layers of accountability.

Regarding technology, although one should acknowledge the importance of advancements, such as those in the field of artificial intelligence, we should understand techno-regulation as the use of technology in guiding and promoting desirable behavior. To that extent, it is more closely associated with "nudging" that with security by design types of solution.

We also affirm that the human element is the most important in promoting cyber hygiene, thus the importance of awareness campaigns, organizational culture and the commitment of top management. Here, we recommend that a clearer association between cyber hygiene, safety, and social responsibility and accountability might increase the levels of cybersecurity within organizations, by attracting a higher commitment on the part of employees.

Reiterating part of the discussion, we recommend that cyber hygiene be directly and more explicitly associated with the vessel's safety and, thereby, framed as an issue of social responsibility and accountability. In other words, similarly to other health and safety issues, and to environmental matters, it might make sense to frame cyber resilience as an area of social responsibility in the maritime shipping industry, and a priority cause for top management, and each employee. This, in a country like Denmark, which prides itself of its levels of digitalization, as well as of its maritime shipping industry, may be an interesting strategy for "cruising digitalization".

Finally, we suggest that these recommendations, as well as the regulatory framework that applies to this case be revised in the near future, in light of coming transformations promoted by automation, and specially the concept of unmanned ships.

REFERENCES

Aalders, Marius and Wilthagen, T. (1997). Moving beyond command-and-control: reflexivity in the regulation of occupational safety and health and the environment. Law and Policy, 19(4), 415–442.

Almklov, P. G., & Lamvik, G. M. (2018). Taming a globalized industry – Forces and counter forces influencing maritime safety. Marine Policy, 96(February), 175–183. https://doi.org/10.1016/j.marpol.2018.08.023

Arduin, Pierre-Emmanuel. (2018). Insider Threats. In Camille Rosenthal-Sabroux (coord.) Advances in Information Systems set. Volume 10. London: Wiley.

Barkenbus, J. N. (1983). Is self-regulation possible? Journal of Policy Analysis and Management, 2(4), 576–588.

Bauer, J. M. and M. J. G. van Eeten. (2009). Cybersecurity: stakeholder incentives, externalities and policy options. Telecommunications policy 33(2009), 706-719.

BIMCO (2019). New Cybersecurity clause from BIMCO. Retrieved on 30 October 2019 at https://www.bimco.org/news/priority-news/20190522-new-cyber-security-clause-from-bimco

BIMCO et al. (2018). The guidelines on cyber security onboard ships. Third version. Produced by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF AND WORLD SHIPPING COUNCIL. Retrieved on 30 October 2019, at https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=20

Black, J. (2001). Decentring Regulation: Understanding the Role of Regulation and Self-regulation in a post-regulatory world. 54 current legal problems, 103.

Boss, Scott R., Laurie J. Kirsch, Ingo Angermeier, Raymond A. Shingler and R. Wayne Boss. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. European Journal of Information Systems (2009), 18, 151-164.

Brownsword, Roger, Eloise Scotford and Karen Yeung (2018). Law, Regulation, and Technology. The field, frame and focal questions. In: ____. The Oxford Handbook of Law, Regulation and Technology. Oxford: Oxford University Press, 3-38.

Centre for Cyber Security (Danish Defense Intelligence Service). (2017). Threat Assessment. The cyber threat against the maritime sector. Retrieved on 28 November 2019, at https://fe-ddis.dk/cfcs/CFCSDocuments/The_Cyber_Threat_to_the_Maritime_Sector_march.pdf

Christiansen, Asbjørn Overgaard. (2018). Interview conducted with Asbjørn Overgaard, head of innovation and Danish Shipping Academy at Danish Shipping, November 13th, 2018, Danish Shipping, Copenhagen, Denmark.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. European Journal of Information Systems, 26(6), 605–641. https://doi.org/10.1057/s41303-017-0059-9

Cyberkeel (2014). Maritime Cyber Risks. Whitepaper.

Danish Defense Intelligence Service. (2017). Intelligence Risk Assessment 2017. An assessment of developments abroad impacting on Danish security. Retrieved on 6 December 2019, at https://fe-ddis.dk/eng/Products/Intelligence-Risk-Assessments/Pages/Intelligence-RiskAssessment-2017.aspx

Danish Maritime Authority (Søfartstyrrelsen) (2017). Analysis of regulatory barriers to the use of autonomous ships. Final report. Produced by Rambøll and Core. Retrieved on 30 October at https://www.dma.dk/Documents/Publikationer/Analysis%20of%20Regulatory%20Barriers%20to%20the%20Use%20of%20Autonomous%20Ships.pdf

Danish Maritime Authority (Søfartstyrrelsen) (2019). Cyber and Information Security Strategy for the Maritime Sector (2019-2022). Danish Maritime Cybersecurity Unit. Retrieved on 30 October 2019 through https://www.dma.dk/Presse/Nyheder/Sider/New-strategy-for-cyber-security-in-the-Danish-maritime-sector.aspx

Danish Ministry of Finance (2018). Danish Cyber and Information Security Strategy (2018-2022). Retrieved on 30 October 2019 through https://digst.dk/media/16943/danish_cyber_and_information_security_strategy_pdfa.pdf

Danish Ship Finance and Rainmaking. (2018). Maritime Trend Report. Retrieved on 30 October 2019, through https://www.shipfinance.dk/media/1910/maritime-trend-report.pdf

Danish Shipping (2018). Shipping companies strengthen their IT security. Retrieved in 30 October 2019, https://www.danishshipping.dk/en/press/news/shipping-companies-strengthen-the-fight-against-cyber-criminals/

Danish Shipping. (2019). Danish Shipping Academy. Introduction to the Shipping Industry. Course. Copenhagen, 25 April 2019.

DeSombre, Elizabeth R. (2006). Flagging Standards: Globalization and Environmental, Safety and Labor regulations at sea. Cambridge: MIT Press.

Dourado, Eli and Jerry Brito. (2012). Is there a market failure in cybersecurity. Mercatus Center. George Mason University. Mercatus on policy series. March 6, 2012.

Dutta, A. and McCrohan (2002). Management's role in information security in a cyber economy. California Management Review 45(1), 670-87.

Ellis Jr., J. O. (Admiral) (2015). Presentation on "Self-regulatory lessons from the US Commercial Nuclear Power Industry: why does it work and why can't it be replicated? CISAC seminar,

05/12/2015, audio file retrieved on 5 February 2019 at https://cisac.fsi.stanford.edu/events/cisac-seminar-admiral-james-o-ellis

European Network and Information Security Agency (ENISA). (2011). Analysis of cyber security aspects in the maritime sector. November 2011.

European Parliament and Council (2016). General Data Protection Regulation. Regulation EU 2016/679 of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrived on 30 October 2019, at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

European Parliament. (2016). Directive on security of network and information systems (NIS Directive). Adopted on 6 July 2016. Retrieved on 30 October 2019. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Fang, B., Ren, K., & Jia, Y. (2018). The New Frontiers of Cybersecurity. Engineering, 4, 1–2.

Friedman, A. (2011). Economic and policy frameworks for cybersecurity risks. Center for Technology Innovation at Brookings, July 2011.

Furger, F. (1997). Accountability and systems of self-governance: The case of the maritime industry. Law and Policy, 19(4), 445–476.

Germond, B. (2015). The geopolitical dimension of maritime security. Marine Policy, 54, 137–142. https://doi.org/10.1016/j.marpol.2014.12.013

Glamsø, Morten. (2018). Interview conducted with Morten Glamsø, senior adviser in the field of security, environment and maritime research at Danish Shipping. November 13th, 2018. Danish Shipping, Copenhagen, Denmark.

Glamsø, Morten. (2019). Interview conducted with Morten Glamsø, senior adviser in the field of security, environment and maritime research at Danish Shipping. May 15th, 2019, Danish Shipping, Copenhagen, Denmark.

Gond, P., N. Kang and J. Moon. (2011). The government of self-regulation: on the comparative dynamics of corporate social responsibility. Economy and Society, 40(4): 640-671.

Greenberg, A. The untold story of NontPetya, the most devastating cyberattack in history. Wired, 13 September 2018.

Groenleer, M., Kaeding, M., & Versluis, E. (2010). Regulatory governance through agencies of the European Union? The role of the European agencies for maritime and aviation safety in the implementation of European transport legislation. Journal of European Public Policy, 17(8), 1212–1230. https://doi.org/10.1080/13501763.2010.513577

Gunningham, N., & Rees, J. (1997). Industry Self-Regulation : An Institutional Perspective, Law and Policy, 19(4), 363-414.

Herath, Tejaswini and H. Raghav Rao. (2009). Protection motivation and deterrence: a framework for security policy. European Journal of Information Systems (2009), 18, 106-125.

Hulgaard, Kasper (2018). Nudging and Cybersecurity. Presentation of Kasper Hulgaard, Behavioral consultant at INudge You, for the Maritime Development Center workshop "Cyber security – threat landscape, trends and employee awareness", Aalborg University Copenhagen Campus, Copenhagen, 1 November 2019.

International Maritime Organization (IMO). (2017b). Guidelines on cyber risk management. MSC-FAL.1/Circ.3 5 July 2017. Retrieved on 30 October 2019. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

International Maritime Organization (IMO). (2019). ISM Code and Guidelines on the Implementation of the ISM Code. Retrieved on 20 October 2019 at http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx

International Maritime Organization (IMO). Maritime Safety Committee. (2017a). Maritime Risk Management in Safety Management Systems. Resolution MSC 428(98), adopted on 16 June 2017. Retrieved on 30 October 2019. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf

IUMI. (2018). IUMI Policy Agenda.

Jensen, Lars. (2018). Interview conducted with Lars Jensen, specialist in cybersecurity within shipping and founder of the consulting Cyberkeel (now part of Improsec Aps). December 3rd, 2019, Copenhagen, Denmark.

Larsen, Jakob (2019). Interview conducted with Jakob Larsen, head of security at BIMCO. April 4th, 2019, BIMCO, Bagsværd, Denmark.

Lessig, L. (1999). Code is law. In: _____. Code and other laws of cyberspace. New York: Basic Books.

Lloyd's Register et al. (2017). Global Marine Technology Trends. Autonomous Systems. Retrieved on 30 October, through https://www.lr.org/th/insights/global-marine-trends-2030/global-marine-technology-trends-2030/

Matten, D. and J. Moon. (2008). "Implicit" and "explicit" CSR. A conceptual framework for a comparative understanding of Corporate Social Responsibility. The Academy of Management Review 33(2): 404-424.

Mital, A. (2015). The unbalanced negative externalities of cybersecurity. The security ledger, May 21, 2015. Retrieved on 31 October 2019, at https://securityledger.com/2015/05/the-unbalanced-negative-externalities-of-cybersecurity/

Munro, K. (2018). Hacking ships. Presentation of Ken Munro, partner at Pen Tester Partners, for the Maritime Development Center workshop "Cyber security – threat landscape, trends and employee awareness", Aalborg University Copenhagen Campus, Copenhagen, 1 November 2019.

Organization for economic co-operation and development (OECD). (2002). OECD guidelines for the security of information systems and networks: towards a culture of security. Retrieved on 30 October 2019 at http://www.oecd.org/sti/ieconomy/15582260.pdf

Organization for economic co-operation and development (OECD). (2012). The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy. Retrieved on 30 October 2019 at http://www.oecd.org/sti/ieconomy/2002-security-guidelines-review.htm

Organization for economic co-operation and development (OECD). Directorate for science, technology and innovation committee on consumer policy. (2015). Industry self-regulation: role and use in supporting consumer interests.

Pahnila, Seppo, Mikko Siponen and Adam Mahmood (2007). Employee's behavior toward IS security policy compliance. Proceedings at the 40th Hawaii International Conference on System Sciences.

Peltier, Thomas R. (2001). Information Security Risk Analysis. New York: Auerbach.

Saunders, M., Phillip Lewis, and Adrian Thornhill (2016). Research methods for business students. Harlow: Pearson Education Limited.

United States, ICS and BIMCO (2019). Measures to enhance maritime security. Submitted to the Maritime Safety Committee at IMO in 26 March 2019.

Von Seleen, M. (2018). Maritime Cyber Threat Landscape. Presentation of Morten Von Seleen, Senior Manager at Deloitte Cyber Incident Response, for the Maritime Development Center workshop "Cyber security – threat landscape, trends and employee awareness", Aalborg University Copenhagen Campus, Copenhagen, 1 November 2019.

Yeung, Karen. 2011. Can we employ design-based regulation why avoiding brave new world? Law, Innovation and Technology, 3(1):1-29.

Wall, Denis S.(2018). Crime, security, and information communication technologies. The changing cybersecurity landscape and its implications for regulation and policing. In: Brownsword, Roger, Eloise Scotford and Karen Yeung (2018). Law, Regulation, and Technology. The field, frame and focal questions. Oxford: Oxford University Press, 1075-1096.

Walters, D., & Bailey, N. (2013). Regulatory Features of the Maritime Industry. Lives in Peril, 98–128.

Walters, D. and Bailey, N. (2013). Managing Health and Safety at Sea. In Lives in Peril (pp. 129–148).

Walters, D., & Bailey, N. (2013). Regulatory Features of the Maritime Industry. Lives in Peril, 98–128.

Winchester, N. and Alderton, T. (2002). Globalisation and de-regulation in the maritime industry. Marine Policy 26 (1): 35-43.

Winner, Langdon. Do artifacts have politics? 1986. In: _____. The Whale and the reactor: a search for Limits in an age of High Technology. Chicago: Chicago University Press.

Zuboff, Shoshana. (2019). The age of surveillance capitalism. The fight for a human future at the new frontier of power. London: profile books.

.

CBS MARITIME

KILEVEJ 14A, 3RD FLOOR, 2000 FREDERIKSBERG, DENMARK
CBSMARITIME@CBS.DK • MAIN: +45 3815 3815
WWW.CBS.DK/MARITIME

CBS COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN