2018-12-06

Cyber-Risk Assessment for Autonomous Ships

Tam, K

10.1109/cybersecpods.2018.8560690
2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)
IEEE

Cyber-Risk Assessment for Autonomous Ships

Kimberly Tam
kimberly.tam@plymouth.ac.uk
University of Plymouth

Kevin Jones
kevin.jones@plymouth.ac.uk
University of Plymouth

***Abstract*—As a $183.3 Billion industry controlling 90% of all world trade, the shipping community is continuously looking for methods to increase profits while still considering human and environmental safety. As a result of developing technologies and policy that make autonomy a feasible solution, at least three separate organizations are aiming to produce and sail their first autonomous ships by 2020. Thus it is essential to begin assessing their cyber-risk profiles in order to rank and mitigate any vulnerabilities. As existing risk models for physical ship safety and autonomous cars do not adequately represent the unique nature of cyber-threats for autonomous vessels within the maritime sector, this article applies a model-based risk assessment framework named `MaCRA` which had previous only been used to model existing ships, not those of the near-future.**

I. Introduction

Due to growing demands on global trade and the resulting economic and environment challenges, various organisations within the maritime community have turned simultaneously toward autonomy to tackle significant challenges associated with ocean-based transportation [1], [2], [3]. The benefits of autonomous ships are multi-fold (e.g., reduces human error [4]), and advances in machine learning, ship sensors, and other related technologies are making this particular solution increasingly feasible and potentially economically viable. For example, some estimate a 90% reduction of annual operation costs with the removal of a ship-based crew [5]. More specifically, these estimates are not of current ship costs with its crew removed, but are calculated specifically for futuristic autonomous ships which, if un-manned, can be stripped of all human-support facilities, systems, and storage required for long manned voyages in potentially extreme conditions.

However, existing cost-effective estimates for autonomous ships disregard the new, potential losses associated with cyber and cyber-physical attacks. The primary reason for this is the current inability to comprehensively assess the risks and vulnerabilities associated with autonomous shipping due to the novel, untested, combinations of sophisticated autonomy technology and traditional maritime systems in a unique, mobile, and economically complex context. Although increased interconnectivity between ships and on-shore infrastructure have improved efficiency, and more is necessary to support autonomous ships, this trend also increases potential cyber-attacks on maritime vessels [6], [7], [8], [9]. To better assess cyber-threats, specifically for autonomous ships, this article extends a novel modelling framework named `MaCRA` (Maritime Cyber-Risk Assessment) [10], which is currently being propagated with today's shipping data, to perform a parallel exploration of the potential cyber-vulnerabilities and associated risks of autonomous ships. Specifically, this article examines three examples of near-future ships, at various stages of autonomy and designed for different purposes, already being prototyped with their first voyage planned for 2020.

- YARA Birkeland: Zero-emission, short-ranged, and fully-autonomous cargo ship by 2020, first prototype in 2018;
- Mayflower Autonomous Ship: Scientific research and experimental technology, first transatlantic voyage in 2020;
- Rolls Royce AAWA: Multi-purpose ocean-travelling "reduced crew" ship in 2020, fully autonomous by 2035.

As the technology and policy for autonomous ships is at a critical point in its development, this article aims to anticipate significant risks and vulnerabilities in the future of autonomous ships based on these three diverse projects and the current cyber-maritime risk landscape. This is somewhat understood as there have been reported cyber-attacks [9], although many have not been released publicly to prevent customers loss [8], [11]. It is also likely that the lack of adequate cyber-training has resulted in the misclassification of cyber-attacks as human error [4], [12]. While the resulting number of maritime-cyber incident reports are relatively low, as there is sufficient data on the system technology being used, and related cyber-attacks, it is possible to calculate autonomous maritime cyber-risks.

The rest of this article is as follows. Section II reviews and propagates the `MaCRA` framework with data related to autonomous ship technology and semantic information. The following Section III uses the model to assess the potential risks of autonomous vessels based on the three diverse examples previously mentioned in an attempt to understand the wider context of maritime cyber-risks and vulnerabilities facing the shipping industry. Section IV discusses related works, before transitioning into the conclusions in Section V.

II. Threat Assessment Framework

In order to assess cyber-risks specific to autonomous ships, this article uses a novel application of the `MaCRA` model, a maritime-specific framework that assess cyber-risks [10]. This model was based on established patterns within threat assessment models [13], [14], [15] but until this point has not been applied to futuristic ships, only present day systems. Hence, this article attempts to extend this model to further the understanding of future cyber-risks associated with autonomous ships by evaluating those threats on three main criteria. Each of the three `MaCRA` axes model one of these criteria, which for the remainder of this paper are as follows:

- $axis_s$: Technological systems and their impacts
- $axis_e$: Attacker ease-of-exploit required for attack
- $axis_r$: Attacker reward for attacking autonomous ships

While the model is often represented visually as 3D or 2D, the model dimension is actually much higher as all three axes are functions of following $attacker$ and $target$ attributes [10].

$$attacker_a = (a_{vector}, a_{goal}, a_{type}, a_{resources}) \quad (1)$$

$$target_t = (t_{vulnerabilities}, t_{effects}, t_{type}, t_{resources}) \quad (2)$$

Hence the MaCRA framework is designed to model an $attacker$'s attack-vector, goal, profile type, and resources. Similarly, $target$ models ship vulnerabilities, possible effects if the vulnerability is exploited, ship type, and defence resources. These attacker and target attributes directly relate to each other, as attack-vectors are derived from target vulnerabilities, and attack impacts are only desirable to an adversary if the targeted system is capable of producing that effect. Furthermore, the types and resources of both parties must be considered together to accurately assess cyber-risk levels.

The remainder of this section demonstrates how MaCRA can be used to specifically model autonomous ships with these attributes and its capabilities for creating comprehensive risk assessment views for a wide range of audiences.

A. System Vulnerabilities and Resulting Impacts

$Axis_s$, as seen in equation (3) of the MaCRA model, is designed to hold the set of maritime systems used by the global fleet, their technological vulnerabilities, and the possible negative impacts (e.g., `AIS jamming : collision`).

$$axis_s = f_{vulnerability}(a_{vector}, t_{vulnerabilities}, t_{effects}) \quad (3)$$

Conversely, in this paper, the subset of systems modelled primarily considers specialized technologies meant for futuristic autonomous operations. Furthermore, the capabilities of these systems define the possible negative impacts that can occur if a modelled system vulnerability is exploited. That said, some environmental factors such as the physical location or ship cargo are also considered, as unique cyber-physical opportunities may occur in specific geological locations [8]. This is particularity relevant to traditionally piracy threats adapting cyber-attack elements, and the mobile nature of ships crossing a number of international borders during its voyages.

1) YARA: The YARA Birkeland is considered the world's first autonomous container feeder with its first voyage planned in 2018 and designed with the intention of being fully autonomous by 2020 [16]. Therefore, for the next few years, three on-shore centres currently handle most aspects of shipping operations such as emergency, operational, and conditional monitoring. Currently this ship has been designed and approved for only two routes between three ports, 7 and 20 nautical miles (nm) apart, and the route never deviates more than 12 nautical miles from the coast. YARA's cargo, specified as fertilizer and chemicals, is also handled autonomously at its designated ports, giving it a unique risk profile to assess.

To first determine levels of ship autonomy, this article defines five tiers in Table I based on SAE definitions for autonomous cars [17]. From this table, it can be surmised that the 2018 prototype is $tier_3$, while the final 2020 version is likely to be $tier_5$, or at least $tier_4$, depending on the environments it can travel autonomously within. In order to perform autonomous sailing, cargo loading/unloading, and mooring functionalities, YARA uses traditional maritime aids (e.g., anti-collision software), communication (e.g., satellite) and automated machinery for cargo and mooring, which is similar to docking. However, its novel battery powered solution and extensive sensor networks are unique, and the degree to which these technologies will be relied on is also significant as decisions will be made primarily with this data. A detailed breakdown of these system vulnerabilities is discussed in Section III, but an overview can be found in Figure 1.

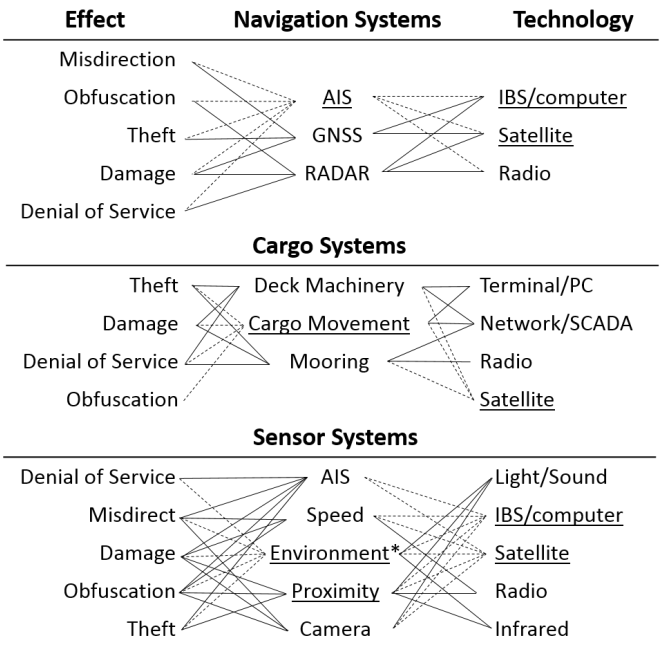

Fig. 1. Mapping of $axis_s$ maritime systems, effects and technology, for near-future autonomous ships (*temperature, light, humidity, orientation ...)

2) AAWA: Rolls-Royce has recently mounted a joint industry project, named Advanced Autonomous Waterbourne Application [18], [19], [20] to research autonomous ships. They have also partnered with Google to develop intelligent awareness software particularly in object recognition [21]. This is necessary, as the planned autonomous ships will host a range of new sensors along with the ship's traditional AIS and radar systems (see Figure 1) [19]. Furthermore, an AAWA white paper does express concerns about hacker activity, particularly around communication and navigation technology, but has not given a comprehensive cyber-risk analysis [18].

As detailed further in the article, each of these technologies have significant cyber-vulnerabilities, and as proposed autonomous ships increase the number of systems for input and guidance (e.g., sensor networks, remote tele-operation communication) and are wholly reliant on these technologies for computer-based decisions, the attack-surface of an autonomous ships is significantly more than traditional ships. Currently there is no published AAWA plans for sailing routes, ship type, or cargo for the 2020 and 2035 checkpoints.

TABLE I
TIERS OF SHIP AUTONOMY, ATTACKER REWARD, AND EoE BASED ON SAE AND MaCRA DEFINITIONS.

	SAE-Based Ship Autonomy	Attacker Reward	Ease-of-Exploit
Tier 1	Minimal crew required and for most, if not all, ship operations.	Little to no value for the attacker. Minimal impact.	Nation State: Advanced Persistent threats, requires nation-level resources.
Tier 2	Partial automation with local crew for simple tasks, e.g. advanced auto pilot.	Small value to attacker.	Corporate: Advanced level attacks requiring considerable resources.
Tier 3	Conditional autonomy, potential interventions by crew.	Average to moderate value for the attacker.	Professional: Moderate level of attack with significant resource investments.
Tier 4	High autonomy, mostly self-running. Local/off-shore crew rarely required.	Valuable to attacker and third parties.	Basic Attack: Minimal skills or resources used.
Tier 5	Complete autonomous ship operations in all potential settings.	Extremely valuable to most players, large-scale or significant impacts.	Little to no skill needed, often uses pre-made exploits (i.e., script kiddies).

3) MAS: Unlike the previous two industry projects, one aimed toward a fully automated ship with limited sailing routes and another researching more widely and further into the future, the Mayflower Autonomous Ship (MAS) project was formed by several groups (e.g., MSubs, ProMare, and University of Plymouth) to develop an autonomous vessel capable of conducting scientific research globally as a platform for new ideas related to maritime autonomy [22], [23]. Thus MAS aims to incorporate a wide range of new technologies for autonomous sailing and scientific research such as newer sensors, new communication technology, smaller autonomous drones for collecting samples, new propulsion systems, and integrating renewable energy for testing in the open sea [22], [24], [25]. While the future design is meant for global exploration, as opposed to the shipping of goods, the first fully-automated voyage (i.e., $Tier_5$) has been planned for 2020 where the ship will sail the same route as the original Mayflower that sailed from England to the USA [23].

With an understanding of these three unique instances of proposed autonomous ships, a larger set of maritime systems likely to appear on any future autonomous ship, regardless of design, can be found in Figure 1. Specifically, these 2D MaCRA model mappings illustrate the connection between system technologies and the possible negative effects that may occur if they are compromised through known, or likely, cyber-vulnerabilities. This data on near-future autonomous ships, modelled by $axis_s$ of the MaCRA framework, differs from the previous study based on existing manned maritime vessels. For example, autonomy reduces the number of on-board navigation systems, traditionally used for human-based operations [10]. However, while reducing the number of systems decreases the attack-surface area, the addition of remote controlled operations in futuristic autonomous ships increase the severity and likelihood of successful exploits.

A more significant increase in risk is shown by the mappings of cargo and sensor systems, as the required communication channels needed for autonomy make these systems much more vulnerable and vastly increases the number of possible impacts during a cyber-attack. Particularly, when compared to the analysis of today's systems [10], the use of satellite is relied upon much more heavily and increasingly central to ship operations. As sensory data was traditionally used by human crew to make better-informed decisions, and since autonomous ships will be solely dependent on this data, these system and their interactions increase the overall attack-surface, decrease attacker effort, and further incentivise maritime cyber-attacks.

B. Attacker Ease-of-Exploit (EoE)

The second axis of MaCRA models the ease-of-effort for an attacker to exploit a vulnerability, which is dependent on their resources and target defences, as shown in equation (4) using attributes from equations (1) and (2). When combined with the other axes, it then becomes possible to assess the risk of a system being exploited and for what negative outcome.

$$axis_e = f_{ease}(a_{type}, t_{type}, a_{resources}, t_{resources}) \quad (4)$$

Traditionally, the experience and awareness of the crew and passengers heavily effect cyber-risks [26], however for autonomous ships, this is not a factor. Although the effects on cost-saving have been viewed for unmanned ships, the associated cyber-risks have not. In an attempt to assess theses risks, this paper makes an addition to MaCRA using Table I for modelling human-based cyber-defences depending on the level of autonomy a ship is classified as. In general, however, while attackers have access to both human and technological resources, targeted autonomous ships will be primarily reliant on technological defences (e.g., firewalls), as remote access is particularly vulnerable due to the mobile nature of ships. Therefore, to deter cyber-attacks, autonomous ship defences must exceed the abilities of an attacker's combined resources, while also considering its location or proximity to casualty or piracy hotspots which could increase the ease of an attack [8].

To model the ease-of-effort (EoE) of attacking a vulnerability, MaCRA uses a five-tier system based on equivalences in conventional computing systems (see Table I). More detailed descriptions of these tiers can be found in the original MaCRA paper [10]. As $tiers_{1-5}$ define the ease of an attack instead of the difficulty, higher tiers represent simpler attacks.

C. Cyber-Attack Reward

Equation (5), $axis_r$, models what an attacker sees as the end-reward value of a cyber-attack. This was designed to assess whether the outcome of an attack is worth an attacker devoting the necessary resources to achieve that goal. Past studies and the MaCRA model have already categorized different cyber-criminal psyches [10], [27], [28], however it seems useful to summarize the most relevant hacker profiles while specifically considering autonomous ships as their potential target. Similar to EoE, MaCRA models attacker incentives using a five-tier reward value system, as seen in Table I.

$$axis_r = f_{reward}(a_{type}, t_{type}, a_{goal}, t_{effects}) \quad (5)$$

Activists, i.e. "hacktivists", often have ideological goals designed to disrupt activities or gain information to alter the behaviour other organizations. Nominally non-aggressive toward people, such attackers may be more destructive towards autonomous ships as there is less risk of harming lives.

Competitors are likely to perform traditional cyber-attacks to extract data for increasing their market influence. However, they may also be more bold with damaging or sabotaging unmanned ships as opposed to manned competitor ships.

Criminals ranging from individuals to organizations traditionally used cyber-attacks to steal or modify data (e.g., for smuggling) or targeted goods at ports and occasionally in transit. If security on autonomous ships are not vastly improved, criminals may be emboldened use cyber-physical attacks to steal goods, ship components, or the ship itself.

Terrorists would not be able to kidnap or blackmail ship personnel on an autonomous ship, but like criminal-types, if the physical-cyber security of the ship is inadequate, they may find smuggling, stealing, or modifying aspects of an autonomous ships to become an asset, or weapon, desirable.

III. Risk Assessment of 2020 Scenarios

With an understanding of how MaCRA can be populated with near-future (i.e. 2020) autonomous ship data, extrapolated from three real-world projects, this section assess the possible cyber-risks and vulnerabilities that will effect the general future of autonomous ships following a more detailed breakdown of the aforementioned systems. As the three examples chosen have diverse designs, and assuming that the majority of futuristic autonomous ships will share commonalities, it can be assumed that they will shall share similar cyber-risks.

Projected risk-assessment views produced by the applied model framework shall be used assess several cyber-attack scenarios. More specifically, MaCRA is able to project risks onto a two-dimensional plane where risk quadrants classify risks into groups (e.g., low, medium, high), as seen in Figure 2. Following that, this article uses MaCRA's quantifier to rank risks categorized as high-risks, or non-acceptable risks, to determine the top risks and their associated technical vulnerabilities for the three examples. Finally, an analysis of common risks across all three examples shall be made to determine likely risks all autonomous ships may face in the near-future.

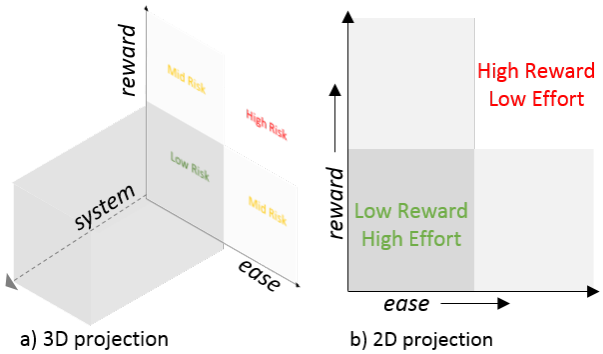

Fig. 2. Projection of MaCRA to risk quadrants for assessing risk.

A. System Vulnerabilities

The **Automatic Identification System** (AIS [29]) was designed to prevent collisions by broadcasting, via marine radio or satellite, ship identity (e.g., name, type), navigation status, heading, position, course, and much more. Typically, marine radio class-B-transponders utilize a combination of GPS and VHF-radio commutation. These technologies already have known cyber-vulnerabilities both in the signals used and their protocols for sending data [26], [30], [31]. Given these vulnerabilities, the risk of adversaries counterfeiting data is real and significant given the reward and effort involved [32]. Based on the types of effects producible by AIS (see Figure 1), criminal and terrorist attacker profiles should have the most interest in these systems. However, unmanned ships may attract more competitors and activists as the likelihood of being caught is considerably lower given the attacker resources are significant enough to obfuscate or hide their activity, e.g, use denial of service (DoS) attack on surveillance.

Global Navigation Satellite System (GNSS) satellites from (1) the USA Global Positional System or GPS, (2) Europe's Galileo, (3) Russian's Global Navigation Satellite System, and (4) China's BeiDou cluster are used in the maritime industry for global position fixing data. In today's modern bridges GNSS is already one of the most interconnected systems. Therefore an autonomous ship that is reliant on increased satellite-based communications to send operation commands and sensory data may be even more vulnerable. This is especially true considering DoS attacks, packet modification, and man-in-the-middle attacks. Moreover, satellite's low-energy signals are a significant technological weaknesses as simple congestion and solar activity can have a significant effect. Therefore active jamming and spoofing [33], [34], [35] are notable vulnerabilities that could present a high-value, low-effort attack. Moreover, loss of GNSS can result in the failure of other ship systems (e.g., AIS) as many are highly dependant on satellite position. As systems on autonomous ships must also be able to receive tele-communications with operational commands from on-shore crew, this increases the attack-surface multi-fold and attacker incentives as a cyber-attack may yield complete control of significant ship operations.

Automated **mooring** was developed to improve physical safety and efficiency during the docking of a ship [36]. As modern mooring technology can be remotely control via radio [36], [37], and is installed in at least two of the examples given [19], [16], radio and networking vulnerabilities are of considerable concern, as attackers interested in delaying operation (e.g., for an individual ship or high-traffic ports), theft, or damage are able to by exploiting these vulnerabilities.

Deck and cargo **machinery** include power winches, cranes, and similar mechanisms for physical operations, such as lowering and lifting anchors. This is particularly relevant to MAS and YARA, as their 2020 plans include the handling of cargo and equipment, e.g. drones. The effects of exploiting these systems nominally include stealing, smuggling, and physical interacting with or damaging nearby entities. Such cyber-attacks are unlikely on today's ships as most are typically manually controlled or locally accessed. However, even today, SCADA-based attacks are possible [38], [39], and so a remote-accessible autonomous ship would possess a greater attack-surface with more possible cyber-risks to consider.

Radio Detection And Ranging (radar) uses radio waves to determine distance and positions of nearby objects [30]. While radio signals are more difficult to jam than satellite, it is still possible [34]. Traditionally, the reward for a radar-based attack is relatively low as a ship is equipped with more relied-upon navigation systems. However, that is based on traditional ships with crews who take information from several sources including visual cues. In comparison, an unmanned ship may be more vulnerable to compromised navigation information. Similarly, without a crew, autonomous ships are likely to be more reliant on their sensors, including radar and similar technologies that emit sound, light, or infrared which may increase the value for exploiting their vulnerabilities.

Sensors for environment, external or internal, and proximity in today's world provide human crews data on temperature, humidity, position, speed, weight, and much more. Internally, sensors are essential for maintaining cargo to prevent explosions, cargo liquefaction, leaks, and cargo damage. This includes, but is not limited to, sensors for chemical, electrical, magnetic, radio, weather, moisture, humidity, flow, fluid velocity, acceleration, light, pressure, density, and temperature.

Technologies such as echo-sounding SONAR, laser-bouncing Lidar (used by YARA, MAS, and AAWA projects), and similar technologies that emit and receive signals share vulnerabilities, such as denial of service. For example, sonar systems are essential for ship operations, as they detect objects under the water for positioning, and while some of the bigger ships often have redundant sonar systems to avoid obstacles, signal congestion can prevent all of them from properly working. Therefore, although future autonomous ships are likely to have larger sets of various sensors for more fine-grained control, as they may all share similar vulnerabilities and communicate with the same systems, all may be compromised with a few, simplistic cyber attacks, unless sophisticated defences are in place. Furthermore, remote crew may be unable to assist, as they may lose access or not be able to differentiate which sensors have been compromised and which, if any, are still providing reliable sensory data. Given how prevalent sensors and sensor networks must be to enable smooth and reliable remote control, autonomous ships are even more likely than today's ships to be targeted, and for a wider range of exploits.

Particularly when considering mid-levels of autonomy, i.e. $tier_{2-4}$, systems using **camera** technology for monitoring should also be considered as potential attack-vectors. In today's shipping industry there already has been a rise in demands for CCTV solutions to monitor ship operations, particularly on large ships with massive storage areas, generators, and important cargo. CCTV technology has known vulnerabilities [40], [41], that could yield rewarding outcomes if a cyber-attacker wishes to obfuscate activity on a ship during cyber or cyber-physical attacks on an unmanned vessel. Moreover if other camera-based systems are developed for internal or external monitoring, the nature of their connectivity to shore-based control centres are likely targets and, if not defended properly, could make autonomous ships vulnerable.

Voyage data recorders (VDR), although not mentioned in Figure 1, may be vulnerable to cyber or cyber-physical attacks to hide other attacker activities. Previous analysis of VDR has showed weak encryption, authentication, firmware update mechanisms, and other dangerous software vulnerabilities that can lead to corrupted or missing data [42]. Analogous to the "black box" for airplane incidences, VDRs collect data from a number of maritime systems for incident reporting. Currently it does not store data relevant for cyber-investigations, but it is likely that fully autonomous and highly technical ships will do so in the future. Also, just as a traditional computer's log can be erased or modified to hide malicious activity, if an autonomous ship's VDR is unprotected, or its future remote-download protocols can be compromised, attackers may target this system to reduce their own risk of being caught.

B. Risk Assessment Projected Views

By propagating `MaCRA` with attacker and target (i.e., YARA, AAWA, MAS) data from the previous sections, it is now possible to asses the risks of these autonomous ships and other future ships hosting similar sets of technology for various levels of autonomy. When fully propagated, the `MaCRA` model can become too complex for effective and comprehensive assessments, therefore projected views are primarily used to analyse the three autonomous examples based on their estimated configurations and operations in 2020. However, with only three targets and four attackers specified, all the data can be shown in Figure 3 along with the systems mapped in Figure 1. The exception is "camera" which was combined with "environment" to create the category "sensor".

From here it is possible to begin analysing the effects of target attributes on their risk profiles. For example, large reward ranges are assigned to YARA, as it may have no cargo (i.e., reward of 0) or be carrying 120 TEUs of fertilizer or chemicals, which may also be valued differently by potential attackers. For example, as a terrorist may find this type of cargo highly valuable (e.g., as weapons material), whereas

	Yara: Short range, *cargo*, coastal, fully-autonomous								MAS: Transatlantic, *research*, fully-autonomous								RR AAWA: Multi-purpose, global reach, reduced crew							
	h_r	h_e	co_r	co_e	cr_r	cr_e	t_r	t_e	h_r	h_e	co_r	co_e	cr_r	cr_e	t_r	t_e	h_r	h_e	co_r	co_e	cr_r	cr_e	t_r	t_e
AIS : Damage	0-1	2-5	1-2	2-5	3-4	4-5	3-5	4-5	0-1	2-4	1-2	2-4	3-4	3-4.5	3-5	3-4.5	0-1	1-3	1-2	1-3	3-4	2-4	3-5	2-4
AIS : DoS	2-3	3-4	2-5	3-4	2	3-4	2	3-4	2-3	3-4	2-5	3-4	2	3-4	2	3-4	2-3	3-4	2-5	3-4	2	3-4	2	3-4
AIS : Misdirect	3-4	3-4.5	3-4.5	3-4.5	3-5	3-5	2-4	3-5	3-4.5	3-4.5	3-5	3-4.5	4-5	3-5	3-5	3-5	3-4	2-3.5	3-4.5	2-3.5	3-5	2-4	2-4	2-4
AIS : Obfuscate	1	3-4	1	3-4	2	3-4	2	3-4	1	3-4	1	3-4	2	3-4	2	3-4	1	3-4	1	3-4	2	3-4	2	3-4
AIS : Theft	1	3-4.5	1	3-4.5	2-4	2-5	3-5	2-5	0-1	3-4.5	4	3-4.5	0-1	2-5	0-1	2-5	0-3	2-3.5	0-3	2-3.5	2-4	2-4	3-5	2-4
Cargo : Damage	**0-2**	3-4	**0-3**	3-4	**0-3**	4-5	**0-4**	4-5	0-2	3-4	0-3	3-4	0-3	3-4.5	0-3	3-4.5	0-2	2-3	0-3	2-3.3	0-3	2-5	0-3	2-5
Cargo : DoS	**0-5**	2-5	**0-5**	2-3.5	**0-2**	3-5	**0-2**	3-5	0-5	2-5	0-5	2-3.5	0-2	3-5	0-2	3-5	0-5	2-5	0-5	2-3.5	0-2	3-5	0-2	3-5
Cargo : Obfuscate	**0-1**	2-3	**0-1**	2-3.5	**0-4**	3-5	**0-3**	3-5	0-1	2-3	0-1	2-3.5	0-4	3-5	0-4	3-5	0-1	2-3	0-1	2-3.5	0-4	3-5	0-4	3-5
Cargo : Theft	***0-3***	4	***0-3***	2-5	***0-5***	4-5	***0-5***	4-5	*1-2*	4	*1*	2-5	*1-2*	4-5	*1-2*	4-5	0-3	2-3	0-3	2-3	0-5	2-4	0-5	2-4
Deck : Damage	1-3	2-3	0-3	2-3	0-3	3-5	0-3	3-5	1-3	2-3	0-3	2-3	0-3	3-4.5	0-3	3-4.5	1-3	1-2	0-3	1-2	0-3	2-4	0-3	2-4
Deck : DoS	2-3.5	2-3	3-4	2-3.5	0-2	3-5	0-2	3-5	2-3.5	2-3	3-4	2-3.5	0-2	3-5	0-2	3-5	2-3.5	2-3	3-4	2-3.5	0-2	3-5	0-2	3-5
Deck : Theft	*0-3*	3	*0-3*	3	*0-4*	4-5	*0-4*	4-5	*1-3*	3	*1-3*	3	*1-3*	4-5	*1-3*	4-5	0-3	2	0-3	2	0-4	4-4.5	0-4	4-4.5
GNSS : Damage	1	2-5	1-2	2-5	3-4	4-5	3-5	4-5	1	2-4	1-2	2-4	3-4	4-5	3-5	4-5	1	1-3	1-2	1-3	3-4	4-5	3-5	4-5
GNSS : Misdirect	3-4	3-4.5	3-4	3-4.5	3-5	3-5	2-4	3-5	3-4.5	3-4.5	3-4.5	3-4.5	4-5	3-5	3-5	3-5	3-4	2-3.5	3-4	2-3.5	3-5	2-4	2-4	2-4
GNSS : Theft	*1*	3-4.5	*1*	3-4.5	*2-4*	2-5	*3-5*	2-5	*1-2*	3-4.5	*2-4*	3-4.5	*2-4*	2-5	*2-4*	2-5	0-3	2-3.5	0-3	2-3.5	2-4	2-4.5	3-5	2-4.5
Mooring : Damage	1-2	3-4	1-3	3-4	1-2	3-4	3-5	2-5	1-2	3-4	1-3	3-4	1-2	*3*	1-2	2-3	1-2	2-3	1-3	2-3.5	1-2	2-3	1-2	2-3
Mooring : DoS	2-5	3-4	3-5	3-4	1-2	3-4	1-2	3-4	2-5	3-4	3-5	3-4	1-2	3-4	1-2	3-4	2-5	3-4	3-5	3-4	1-2	3-4	1-2	3-4
Mooring : Theft	*0-3*	3-4	*0-3*	1	*0-4.5*	3-4	*0-4.5*	3-4	*0*	3-4	*0-1*	1	*1*	3-4	*1*	3-4	0-3	2-3	0-3	2-3	0-4.5	1-2	0-4.5	1-2
Proximity : Damage	0-1	3-5	1-2	3-5	3-4	4-5	3-5	4-5	0-1	3-4.5	1-2	3-4.5	3-4	4-5	3-5	4-5	0-1	2-3.5	1-2	2-3.5	3-4	3-4	3-5	3-4
Proximity : Obfuscate	1-2	3	1-2	3	1-2	3	2-5	2-3	1-2	3	1-2	3	1-2	3	2-5	2-3	1-2	3	1-2	3	1-2	3	2-5	2-3
Proximity : Theft	*1-3*	3-4	*1-3*	1	*1-2*	3-4	*1-2*	3-4	*1-3*	3-4	*1-3*	1	*1-2*	3-4	*1-2*	3-4	0-3	2-4	0-3	2-4	0-3	2-3	0-3	2-3
Radar : Damage	1	3-5	1	3-5	3-5	3	1	3	1	2-3	1	2-3	3-5	*3*	1	*3*	1	1-2	1	1-2	3-5	2	1	2
Radar : DoS	2	2	2-3	2	2	2-3	2	2-3	2	2	2-3	2	2	2-3	2	2-3	2	2	2-3	2	2	2-3	2	2-3
Radar : Obfuscate	1-2	3	1-2	3	1-2	3	2-5	2-3	1-2	3	1-2	3	1-2	3	2-5	2-3	1-2	3	1-2	3	1-2	3	2-5	2-3
Sensor : Damage	0-1	3-5	1-2	3-5	3-4	4-5	3-5	4-5	0-1	3-4.5	1-2	3-4.5	3-4	3-4	3-5	3-4	0-1	2-3.5	1-2	2-3.5	3-4	3-4	3-5	3-4
Sensor : DoS	2-3	2-3	1	2-3.5	2	2-4	2	2-4	2-3	2-3	1	2-3.5	2	2-4	2	2-4	2-3	2-3	1	2-3.5	2	2-4	2	2-4
Sensor : Misdirect	3-4	3-4.5	3-4	3-4.5	3-5	3-5	1-2	3-5	3-4.5	3-4.5	3-4.5	3-4.5	4-5	3-5	2-5	3-5	3-4	2-3.5	3-4	2-3.5	3-5	2-4	1-2	2-4
Sensor : Obfuscate	1	3-4	1	3-4	2	3-4	2	3-4	1	3-4	1	3-4	2	3-4	2	3-4	1	3-4	1	3-4	2	3-4	2	3-4
Sensor : Theft	*0-3*	4	*0-3*	2-5	*0-3*	4-5	*0-3*	4-5	*1-2*	4	*1-3*	2-5	*2-4*	4-5	*2-4*	4-5	0-3	2-4	0-3	2-4	0-3	1-2.5	0-3	1-2.5
Speed : Damage	0-1	3-4.5	1-2	3-4.5	3-4	4-5	3-5	4-5	0-1	3-4.5	1-2	3-4.5	3-4	3-4	3-5	3-4	0-1	2-3.5	1-2	2-3.5	3-4	3-4	3-5	3-4
Speed : Misdirect	1-2	3-4.5	2-4	3-4.5	3-5	3-5	2-3	3-5	1-2	3-4.5	2-4	3-4.5	3-5	3-5	2-3	3-5	1-2	2-3.5	2-4	2-3.5	3-5	2-4	2-3	2-4
VDR : Obfuscate	1-2	3-5	3-4	3-5	4-5	4-5	4-5	4-5	1-2	3-5	3-4	3-5	4-5	4-5	4-5	4-5	1-2	3-4	3	3-4	4	4	4	4

Fig. 3. Risk tier values (Section II) for all hacker profiles against the systems of near-future (i.e., 2020) versions of three proposed autonomous ships.

a local competitor may not. However, as the YARA has a short, coastal route in Norway which (1) is not a known terrorist hotspot and (2) is close to the local authorities, this may present a low EoE for attackers both foreign and domestic. Similarly, MAS is designed to carry cutting-edge research technology, making them or their components a more likely target than the samples (e.g., soil) it holds as cargo. Furthermore, the transatlantic route of MAS's first 2020 voyage does not take it through any known terrorist or criminal hotspots. However, as both MAS and YARA traverse narrow channels, this may increase the EoE for land-based attacks or causing collisions with other ships or natural obstructions.

Lastly, while less is known of the AAWA 2020 ship type, cargo, and operations, it is known that the prototype shall have $tier_2$ autonomy, as a reduced crew will be present. As the crew of an experimental ship is likely to be well trained and alert, this could significantly improve the ship's defences against misdirection, theft and damage. In comparison, higher-tiered autonomous ships will be designed to solely rely on computer-based decision making. Lastly, as these are incomplete projects, areas lacking detail use ranges to create MaCRA risk zones, and occasionally if absolutely no information is provide, like with cyber-defences, the examples are assumed to have the same as equivalent ships today.

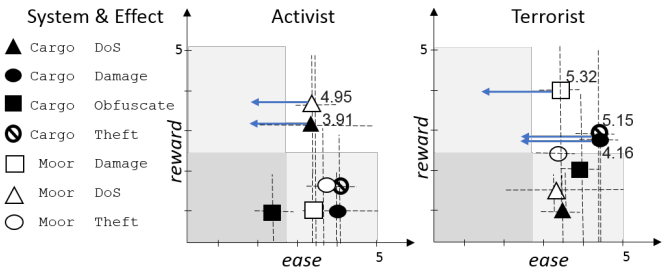

Fig. 4. Hactivist and Terrorist risks for Yara ship-port systems.

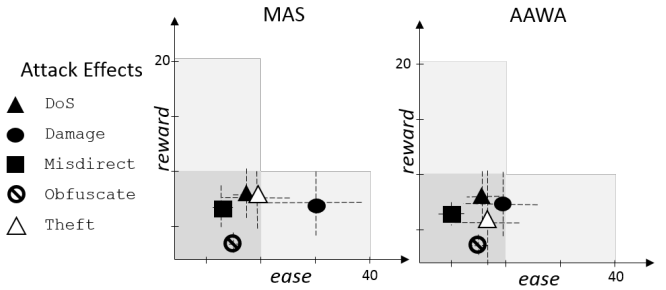

Fig. 5. Summed effect-focused risks for competitor attackers.

Different projected views can be made from the same underlying data to contextualize the risks of autonomous ships. In Figure 4, which projects a specific risk scenario by filtering out data irrelevant to the desired assessment, the three ports on the autonomous YARA ship's route wish to assess ship-to-port cyber-physical risks by only analysing the relative systems, namely mooring and cargo. Moreover, the assessors are specifically interested in the risks associated with a range of activist and terrorist groups. Once the irrelevant data has been filtered out and the projected view has been produced, it is then possible to simulate the effects of additional security and view the resulting shifts on the same risk projection.

As seen in Figure 4, ranges of reward and EoE tier values are depicted by dotted lines. These outline the boundaries of risk zones, accounting for worst to best case scenarios and changes in attributes, such as whether the target is currently carrying cargo or not. Specifically, when considering the risk of YARA loaded with its cargo, the risks may shift toward the top of their range, transitioning some risks from mid-level to high. Once projected onto risk quadrants, assessors can quickly determine that the top risks or main concerns are DoS by activists and theft by terrorists (see Figure 4). Thus, increased security in the local port areas shall lower the risks, as shown with arrows. Later, as attackers evolve those risks may rise again. Lastly, aside from risk zones and quadrants, MaCRA can quantify and rank risks with a risk indicator function [10], as shown with the high-level risks in Figures 4 and 6.

The second assessment compares risks to MAS and AAWA with Figure 5. Specifically, as these are cutting-edge ships about to be sent on transoceanic voyages, the assessor wants to determine the risks from competing companies also developing autonomous shipping technology. Furthermore, instead of assessing risk per individual system, this assessment determines what the most likely cyber-attack outcomes could occur, disreguariding the system that caused it, by summing the risks related to each impact. This projected view pushes outcomes that can be achieved through several system vulnerabilities toward higher-risk quadrants. As no high risks from competitors is found with Figure 5, no risk values are shown. However, if the assessor wishes, the threshold can be lowered (i.e., reduce grey box size) to redefine thresholds for low, mid, and high risks. While the risk profiles for MAS and AAWA are similar, as they model the same attacker, factors such as AAWA's reduced crew introduce variances in damage and theft risks.

Lastly, to assess general, yet significant, cyber-risks facing future autonomous ships, Figure 6 sums the risks for all attackers, targets, and systems in Figure 3. This projection reflects three diverse examples of autonomous ships and pushes systems with multiple vulnerabilities and negative impacts into the high-risk zone, which MaCRA then ranks. Therefore, based on near-future autonomous ship designs, the most at-risk systems for the future are AIS, GNSS, and growing interconnected networks of sensors. As for highlighting essential solutions, all projected views and assessments demonstrate that safe protocols for remote satellite-based communications can drastically decrease risks for future autonomous ships.

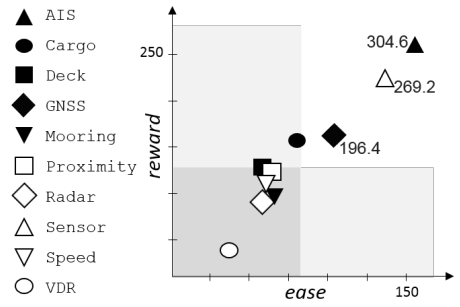

Fig. 6. Combined risk profile predictions for future autonomous ships.

IV. Related Work

This article does not predict generic statistics-based risks [43], [44], [45] or maritime-cyber risks facing existing ships [10], but those specific to the future of autonomous maritime ships. This is becoming increasingly important, as the associated technology, laws, and economy continues to evolve in anticipation of significant breakthroughs within the next few years [5], [18], [22]. Moreover, the purpose of this study is not to identify specific vulnerabilities within individual systems or autonomous algorithms [26], [31], [32], [35], [46] but instead seeks to understand the cyber-maritime risks that will arise when all these systems are connected on the first fully-autonomous and widely used ships. While cyber and cyber-physical security are notable concerns [18], no existing solution has achieved a comprehensive understanding of the new cyber-risk landscape. Hence this study aimed to better define and quantify those risks, so that future research can address those identified areas of high-risk and vulnerability.

Based on the above, it is the authors' understanding that majority of today's maritime-cyber research focuses on (1) individual technological systems, not as a collection of interconnected systems [32], [47], [48], [49], and (2) the risk or vulnerability of today's technology, with a particular focus on navigation-based systems [42], [50], [51]. Furthermore, in the specific area of autonomous ships, most pre-analysis or early research claim that cyber-security is a top concern [18], [52], but do no attempt to understand the full maritime-cyber risk landscape for future autonomous ships, as this article aimed to do with the novel application of the MaCRA risk model.

Although there are overlaps in autonomy research with cars and airplanes [53], [54], [46], just as the risk profiles and models differ between planes and cars [53], [54], [55], [56], variations in technology and environment dictate that any model used for ocean-based targets need to be equally sensitive to the relevant factors, which the applied MaCRA framework does. However, unlike the original MaCRA study, this article uses the model to assess risk in a subset the future global fleet. Furthermore, while this study focuses on autonomy at a critical time in its development, it is not limited to only attacker assessments [57], [58], the aforementioned system-focused studies, or risks limited to geological regions [59].

V. Conclusions

This article performs a novel and necessary risk analysis on the future of autonomous ships based on three near-future prototypes currently in progress. These examples, with significant 2020 checkpoints, exemplify different futuristic autonomous ships and allow us to begin understanding upcoming maritime-cyber risks and vulnerabilities, particularity those pertinent to cutting-edge sensor networks and remote access. Although modelling data is currently sparse, this is the first analysis to assess autonomous ships at this scale and level of detail in order to guide future cyber-secure maritime autonomy. Moreover, as autonomy developments continue to advance as discussed, the `MaCRA` model can be dynamically updated to assess the new risk landscape, making it a powerful, adaptive tool for assessing cyber-risks as shipping continues to evolve.

References

[1] International Chamber of Shipping (ICS), "Shipping, world trade and the reduction of CO2 emissions," *United Nations Framework Convention on Climate Change (UNFCCC)*, 2016.

[2] ——, "Review of maritime transport," *United Nations Conference on Trade and Development (UNCTAD)*, 2016.

[3] Food and Agriculture Organization of the United Nations, "The state of world fisheries and aquaculture," OECD-FAO publication, 2014.

[4] A. Rothblum, "Human error and marine safety," International Workshop on Human Factors in Offshore Operations (HFW2002), 2000.

[5] D. MORRIS, "Worlds first autonomous ship to launch in 2018," http://fortune.com/2017/07/22/first-autonomous-ship-yara-birkeland/, 2017.

[6] K. Jones, K. Tam, and M. Papadaki, "Threats and impacts in maritime cyber security," IET Engineering & Technology Reference, 2016.

[7] USMRC MCAT, "The reality of shipboard cyber vulnerabilities," USMRC Maritime Cyber Assurance Team, 2016.

[8] Allianz Global Corporate and Specialty SE, "Safety and shipping review 2016," Allianz Global Corporate and Specialty, 2016.

[9] Maersk, "A. P. Moller Maersk improves underlying profit and grows revenue in first half of the year," *Maersk*, Aug 2017. [Online]. Available: https://www.maersk.com/en/press/press-release-archive

[10] K. Tam and K. Jones, "MaCRA: A model-based framework for maritime cyber-risk assessment," UoP Technical Report, 2018.

[11] W. Cassidy, "China-based cyberattack hits logistics operators, shippers," Outsource, volume 5 issue 6, 2017.

[12] M. Wingrove, "Lack of training causes ship accidents and detentions," Marine Electronics & Communications, 2016.

[13] United States General Accounting Office, "Information security risk assessment practices of leading organizations," GAO/AIMD-98-68, 1999.

[14] T. Peltier, "Information security risk analysis," Auerbach Publ., 2005.

[15] R. Borgovini, S. Pemberton, and M. Rossi, "Failure mode, effects, and criticality analysis (FMECA)," Reliability Analysis Center, 1993.

[16] K. Maritime, "Autonomous ship project, key facts about YARA birkeland," https://www.km.kongsberg.com/, 2017.

[17] SAE International, "Automated driving," SAE J3016, 2016.

[18] AAWA, "Remote and autonomous ship," white paper, 2016.

[19] Rolls-Royce, "Technology development areas in AAWA," http://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/2%20Technology%20-.pdf, 2016.

[20] O. Levander, "Forget autonomous carsautonomous ships are almost here," https://spectrum.ieee.org/transportation/marine/forget-autonomous-cars-autonomous-ships-are-almost-here, 2017.

[21] Rolls-Royce, "Rolls-royce joins forces with google cloud to help make autonomous ships a reality," https://www.rolls-royce.com/media/, 2017.

[22] Shuttleworth, "Mayflower autonomous research ship," http://www.shuttleworthdesign.com/gallery.php?boat=MARS, 2018.

[23] Mayflower400, "Explore the mayflower trail," http://www.mayflower400uk.org/, 2018.

[24] S. Sensing, "Silicon sensing supports 'mayflower' autonomous ship project," https://www.siliconsensing.com/press/mas400/, 2018.

[25] ShipTechnology, "Mayflower autonomous research ship (mars)," http://www.ship-technology.com/projects/, 2018.

[26] CyberKeel, "Maritime cyber-risks," NCC Group Publication, 2014.

[27] BIMCO, CLIA, ICS, INTERCARGO, and INTERTANKO, "The guidelines on cyber security onboard ships version 2.0," ICS, 2016.

[28] C. Fitch, "Crime and punishment: The psychology of hacking in the new millennium," SANS Institute, 2004.

[29] International Maritime Organization, "Solas chapter V annex 17: Automatic identification systems (AIS)," IMO, 2004.

[30] U. N. Archives and R. Administration, "CFR Title 47 (parts 80-end) code of federal regulation title 47 telecommunications revised as of october 1, 2016," Code of Federal Regulations (CFR), 2016.

[31] G. Mordechai, G. Kedma, A. Kachlon, and Y. Elovici, "Airhopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies," Malicious & Unwanted Software Conference, 2014.

[32] J. Wagstaff, "All at sea: Global shipping fleet exposed to hacking threat," Reuters, 2014.

[33] US Department of Homeland Security, "Gps and critical infrastructure," Civil GPS Service Interface Committee, 2015.

[34] J. Coffed, "The threat of gps jamming," Exelis, 2014.

[35] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the gnss spoofing threat and countermeasures," *ACM Comput. Surv.*, 2016.

[36] Cavotec, "Moormaster frequently asked questions," Cavotec, 2014.

[37] M. MOOREX, "Mooring and auto-mooring solutions," ShipServ, 2014.

[38] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in scada networks," Computers & Security.

[39] J. Leyden, "Water treatment plant hacked, chemical mix changed for tap supplies," The Register, 2016.

[40] A. Costin, "Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations," in *Proceedings of the 6th International Workshop on Trustworthy Embedded Devices*, 2016.

[41] C. Heffner, "Exploiting surveillance cameras like a hollywood hacker," Tactical Network Solutions, 2013.

[42] R. Santamarta, "Maritime security: Hacking into a voyage data recorder (VDR)," IOActive, 2015.

[43] F. Goerlandt and J. Montewka, "Maritime transportation risk analysis: Review and analysis in light of some foundational issues," *Reliability Engineering & System Safety*, 2015.

[44] J. Montewka, S. Ehlers, F. Goerlandt, T. Hinz, K. Tabri, and P. Kujala, "A framework for risk assessment for maritime transportation systemsa case study for open sea collisions involving ropax vessels," *Reliability Engineering & System Safety*, 2014.

[45] J. Nordstrm, F. Goerlandt, J. Sarsama, P. Leppnen, M. Nissil, P. Ruponen, T. Lbcke, and S. Sonninen, "Vessel triage: A method for assessing and communicating the safety status of vessels in maritime distress situations," *Safety Science*, 2016.

[46] C. Berger and B. Rumpe, "Autonomous driving - 5 years after the urban challenge: The anticipatory vehicle as a cyber-physical system," *CoRR*, 2014.

[47] Marine accident investigation branch, "Grounding of CSL THAMES in the Sound of Mull," Marine accident investigation branch, 2012.

[48] ——, "Report on the investigation of the grounding of Ovit in the Dover Strait," Marine accident investigation branch, 2014.

[49] Y. Vandenborn and R. Bell, "Standard safety special edition - ECDIS assisted grounding," Marine accident investigation branch, 2015.

[50] CyberKeel, "Security risks and weaknesses in ecdis systems," NCC Group Publication, 2014.

[51] Y. Dyryavyy, "Preparing for cyber battleships: Electronic chart display and information system security," NCC Group Publication, 2014.

[52] M. Blanke, M. Henriques, and J. Bang, "A pre-analysis on autonomous ships," Technical University of Denmark DTU Electro, 2018.

[53] C. A. T. Control, "Cyber security project," www.csfi.us, 2015.

[54] D. Snyder, J. Powers, E. Bodine-Baron, B. Fox, L. Kendrick, and M. Powell, "Improving the cybersecurity of u.s air force military systems throughout their life cycles," RAND corporation Research Report, 2015.

[55] G. Yeomans, "Autonomous vehicles handing over control: Opportunities and risks for insurance," Lloyd's, 2014.

[56] C. Bordonali, S. Ferraresi, and W. Richter, "Shifting gears in cyber security for connected cars," McKinsey&Company, 2017.

[57] Danish Defence Intelligence Sevice's Center for Cyber Security (CFCS), "Threat assessment: The cyber threat against the maritime sector," Marine Cyberwatch, 2014.

[58] JHC and S. Harwood, "Cyber risk," Joint Hull Committee, 2015.

[59] S. Bateman, "Regional maritime security: threats and risk assessments," University of Wollongong, 2010.