MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment

Kimberly Tam and Kevin Jones
University of Plymouth

April 3rd 2018
Technical Report#: CSCAN.2018.TR.01

CSCAN
WITH
PLYMOUTH
UNIVERSITY

MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment

Abstract

In today's economy roughly 90% of all world trade is transported by seagoing vessels. Varying ship functionality, configuration, and cargo type have created a diverse set of specialized ships including, but not limited to, leisure passenger crafts, naval fleets, oil tankers, and cargo carriers. Whilst the global fleet utilizes a plethora of technology, the vast majority share similar systems for core functionalities such as navigation, communication, and propulsion. As existing risk models do not adequately represent the unique nature of cyber-threats in the maritime sector, this article introduces a model-based risk assessment framework which considers a ship's technological vulnerabilities, potential attackers, and possible attacker incentives and impacts, with the intention of aiding operators, regulators, insurers, and crew in quantifying and mitigating maritime cyber-risks with optimal resource spending.

I. Introduction

Despite the growing number of economic and environmental challenges in international shipping, the vast majority of global trade both in volume and value is still conducted on the ocean [1], [2], [3]. While a significant percentage of the global fleet consists of bulk carriers and oil tankers, there is still a wide variety of ships designed for passengers, fishing, services (e.g., ice breakers), specialized cargo, military, and scientific exploration [2], [3]. In response to the number of diverse factors involved in ocean travel (e.g., ship type, configuration, cargo, route, crew), many technologies have been standardized to provide international standards for navigation, traffic control, cargo management, propulsion, and monitoring. Such novel combinations of on-shore and maritime technology, and a unique, mobile context, creates interesting cyber-risk scenarios in which traditional attackers and new cyber-attackers may find increased profits with less risks.

While increased interconnectivity between ships, personal devices, and on-shore infrastructure has improved efficiency and physical safety, it has also enabled an increase of cyber-attacks on maritime vessels and related structures [4], [5], [6], [7]. To better assess cyber-threats within the maritime sector, and (1) accurately characterize maritime-cyber risks and their severity across the global fleet (2) provide risk data in useful projected views to support policy makers, ship insurers, shipping companies, etc. and (3) identify key technological systems requiring further cyber-security research, this study proposes a novel modeling framework named `MaCRA` (Maritime Cyber-Risk Assessment), which we illustrate with example system and attacker data. To highlight the plausibility of intentional cyber-attacks on the system vulnerabilities identified in this article, real-life accidents that occurred due to the same flaws are also presented. This has significance, as it has been difficult to obtain general statistics on all cyber-related maritime incidents. This is because many of the small-scale attacks currently go unnoticed (e.g., stolen personnel or shipping data) and some of the more significant attacks have not been released publicly to prevent loss of customers [6], [8]. It is also our belief that the lack of adequate cyber-training often results in the misclassification of cyber-attacks as human or machine error [9], [10].

While the majority of maritime cyber-crimes lack the sophistication and magnitude of on-shore attacks, continuing trends of powerful, networked systems in a lucrative global market demands a proactive approach toward maritime cyber-risks. Moreover, based on the global fleet's development, understanding the threats against today's most technologically advanced ships may better protect emerging ships of the future (e.g., autonomous ships [11], [12]). While technology

change also increases maritime accidents [6], that is not the focus of this study (see Section V). This article examines maritime cyber-risks by using a model-based approach than can assess all, even zero-day, risks in multiple contexts and scenarios. Specifically, this article aims to:

- Provide an overview of the MaCRA framework and how it models maritime cyber-risk variables including attacker incentives and a ship's changing environment in Section II;
- Systematically breakdown popular ship system technologies, including analyses of both known and theoretically plausible cyber-vulnerabilities, in Section III;
- Populate the proposed MaCRA model with data discussed previously (e.g. attacker and system variables) and exhibit several use-case scenarios and assessments in Section IV.

The rest of this article is as follows. Section II describes the proposed MaCRA concept, a unique, model-based, risk assessment framework designed specifically for the maritime environment. Next, the article evaluates several sets of system vulnerabilities found on real-world ships, along with related incidences (see Section III), and demonstrates several MaCRA use-cases through a series of illustrative assessments in Section IV. This article does not evaluate an exhaustive set of maritime systems, but is sufficient to demonstrate MaCRA's abilities. The MaCRA framework is then compared to related works, both in maritime-cyber security and the risk assessment sector (see Section V). Sections VI and VII conclude with possible research paths for future work, including populating the MaCRA model with more complex industry data, and how this work can benefit the extensive shipping industry (e.g., economically, cyber-security).

II. Threat Assessment Framework

Based on the well established pattern of general risk and threat assessment models [13], [14], [15], this article attempts to gain a better understanding of ship cyber-risks by evaluating threats on three main criteria: (1) System vulnerability and effect (2) ease-of-exploit (later referred to as EoE or "ease") and (3) end result or "reward". These three are modeled as a 3D matrix, with each aspect assigned an axis, labeled as $axis_1$, $axis_2$, and $axis_3$ respectively. To this end, MaCRA aims to increase general cyber-awareness and to assist the maritime community (e.g., ship operators, regulators, insurers, manufactures) in strategically reducing their cyber-risks against both known and theoretical threats using detailed risk assessment shown in projected views.

Depending on what an analyst is assessing, different subsets of the underlying data can be extracted from MaCRA to create intuitive views. More specifically, to make the results more intuitive for a wider audience, MaCRA is capable of reducing model complexity by projecting views for assessments and comparing the maritime-cyber risks of individual ship systems, entire ships, and any sized fleet of ships. Given EoE and reward axes, analysts may also compare risks with different attacker and target attributes, such as the attacker's incentives, sophistication, or resources. This is one powerful capability for analyzing risk, based not just on the physical ship, but its function and environment, as demonstrated further in the following sections.

A. Vulnerability Characteristics

$Axis_1$ of the MaCRA framework enumerates a set of system vulnerabilities to be modeled and their possible negative impacts (e.g., `GPS spoofing : ship misdirection`). While generating a complete set of all technological vulnerabilities and their effects for the entire global fleet is outside the scope of this paper, and as no set already exists, the authors were able to obtain sufficient real-world data on maritime systems in Section III to showcase the proposed MaCRA framework. Although $axis_1$ is primarily affected by a ship's on-board technology, it is important to note that environmental factors (e.g., ship geographical location, crew) are significant variables that are also accounted for. For example, crew members can be blackmailed or targeted

TABLE I
EASE OF EXPLOIT (EoE) WITH RESPECT TO ATTACKER ABILITIES AND RESOURCES.

Tier	Human-based Resources	Technological Resources
$Tier_5$: Script Kiddy	Little to no skills, often uses existing exploits and tools. Attacks are non-adaptive if it fails. Often leaves forensic evidence and is detectable because of simplicity.	Knows what low-level tools are available, how to obtain, and known vulnerabilities.
$Tier_4$: Basic Attack	Some preparation (e.g., time) needed to target a single vulnerability (one with little to no protection). Often leaves forensic evidence and is detectable because of simplicity.	Able to trade for better attacks or has resources to create/alter known attacks.
$Tier_3$: Professional	Preparation (e.g., time) needed to target a single vulnerability with has basic protection. May leave forensic evidence. May create "families" of similar attacks and known patterns.	Has solid knowledge and/or external assistance for generating/testing attack.
$Tier_2$: Corporate	One or more advanced systems affected, despite target defenses. May not leave forensic evidence, some aspects difficult to detect. Requires significant preparation (e.g. time).	Resources for understanding/nullifying some defenses + $Tier_3$ knowledge.
$Tier_1$: Nation State	Advanced Persistent Threats (APT), one or several systems can be targeted simultaneously to achieve goals. Target is well protected with strategic, effective defenses. May not leave forensic evidence, most aspects difficult to detect, and requires long-term planning.	Resources include advanced tools, self-made or outsourced, tools to obfuscate attack and bypass defenses.

by email phishing attack vectors [16], and some physical locations provide unique opportunities for certain attacks, making MaCRA applicable to complex socio-technical scenarios like insider threats and sensitive to global factors, e.g. aspects of the economy tied to maritime-based trade.

The need for accurate cyber-risks assessments is becoming more critical to ensure economic and physical safety as maritime systems grow more technologically dependent and advanced. With the advent of satellite positioning, key systems such as navigation are becoming even more centralized on a ship, creating an Integrated Bridge System (IBS). The IBS enables easier control and monitoring functions by providing an information-rich area with increasingly fine-grained controls. Typical system components of the IBS can be divided by functionality; navigation, control, communication, machinery management, cargo management, safety, crew welfare, and specialized systems [16]. Furthermore, the IBS often provides an Internet gateway, allowing access to external systems and entities. Section III explores IBS system categories in detail.

B. Ease-of-Exploit (EoE)

Semantic, environmental factors play a much more central roll in modeling $axis_2$ when determining the EoE of each system and its achievable effects. For example, the experience and awareness of the crew and passengers could deter or allow a cyber-attack [17]. Moreover, it is also likely that a ship's configuration (e.g., firewalls) and physical location could determine the likelihood of an attack. For example, close proximity to shipping casualty or piracy hotspots would imply attack advantages at those coordinates [6]. Furthermore, if damage is the attacker's goal, certain ports and areas with physical obstructions (e.g., sandbars) would increase EoE.

Unlike $axis_1$, which focuses on modeling the ship systems, the purposed $axis_2$ and $axis_3$ determine how likely an attacker is to exploit a vulnerability and trigger its possible effects. The EoE or "ease" axis is used to model the level of resources a hacker must expend, relative to their capability, to successfully perform an attack. Modeling this data in MaCRA, the EoE of a system is determined by the difficulty level of attacking its vulnerability. To this end, MaCRA uses a five-tier system based on equivalences in conventional computing systems to represent the level of "hacking ability" and available resources required for the desired exploit (see Table I). The tiers descend in number, as MaCRA plots the EoE. For example, if the GPS on a vessel is

vulnerable to both jamming and spoofing, the latter is more complex with a higher "cost" for the attacker, so MaCRA may assign it an EoE score of $tier_3$ or $tier_4$, depending on the ship defenses. In contrast, jamming can be achieved with little to no understanding of the technology involved, and so has a higher EoE score of $tier_5$.

The contents of Table I primarily considers the EoE of intentional attacks, however they may also equate to accidental or unintentional impacts, such as leaking sensitive information without fully comprehending the results. When discussing attacker profiles (e.g., activists) this aspect will be taken into account, as one cyber-attack could open back doors or leak information that may not initially seem important. While MaCRA is able to determine risks of intentional attacks to achieve known goals, it may not be as accurate, and therefore effective, for accidental outcomes (see Section V). Although a limitation, such a risk may updated afterwards by mapping the same EoE factor with an increased attack reward value, or visa versa, to improve the model data.

C. Cyber-Attack Reward

$Axis_3$ of the MaCRA framework models the end-reward value, as seen from the attacker's perspective. This modeling of attacker incentives determines whether the outcome of an attack is desirable enough for an attacker to invest the necessary resources. To fully understand this aspect of the cyber-criminal psyche, MaCRA must correctly model the types of attackers and their motivations. The following closely mirrors traditional cyber-attacker profiles within existing standard security landscape [16], [18].

Activists: Also known as "hacktivists", the desired outcome of activist groups is to achieve ideological goals. This often results in attacks designed to disrupt activities or gain, and publicize, information to alter the behavior of their targets. While nominally non-aggressive, their activities may create opportunities that benefit other attackers or cause accidental damage or leaks. In the maritime ethos, activists typically desire environmental or political-based impacts.

Competitors: Competing companies, or even opposing nations, may seek to increase their own market influence in the global economy through cyber-crime. In most non-extreme cases the desired goal is to acquire information, such as the opponent's current bids, shipping manifests, and customers, to be utilized in corporate settings. However, there is also incentive for disrupting a competitor's ship operations to damage financial status or reputation.

Criminals: These attackers range from individuals to groups of varying size and sophistication. The vast majority of criminals desire profit in one form or another including physical and intellectual theft, fraud, smuggling, blackmail, and extortion. At one end of the spectrum, simple cyber-attacks may be used to increase the effectiveness of typical physical crimes (e.g., piracy [19]), while at the other end there is the increase in organized-crime, with groups developing and selling cyber-tools to all types of attackers (i.e., indirect profit) [20].

Terrorists: While the previous cyber-attackers may occasionally cross a line or cause unintentional impacts that result in unnecessary deaths or damage, terrorists using cyber or cyber-physical attacks often actively seek this result. In addition, this attacker type may desire to increase their member count and resources, which may result in theft, the spread of propaganda, and blackmail. In a more sophisticated attack, the ships themselves may become an asset for long distant cyber or physical attacks that may cause local or global damage.

Elitist/Prankster: In a small niche of today's hacking community, elitists traditionally hacked systems to test, or show-off, their knowledge and skills. Regardless of the decline in such non-profit hackers, we choose to exclude elitists from the MaCRA model because elitist attacks rarely exhibit negative outcomes [18]. Furthermore, we consider pranksters as a subset of, mostly low-level, criminals although they may be more "mischief" driven than criminally profit-driven.

TABLE II
LEVELS OF CYBER-ATTACK REWARDS AS SEEN BY ATTACKER

Tier 1	Little to no value: Target outcome can be accomplished with little or no exploit effort and results are minimal both to the attacker(s) and to 3^{rd} parties (e.g., black market).
Tier 2	Small value: Low level attacker (i.e., $tier_{1-2}$), small impact in quantity and scale, (i.e., secondary effect of main attack).
Tier 3	Average value: Outcome is primarily valuable to attacker(s), not a 3^{rd} party, and may fulfill the attacker's goal.
Tier 4	Valuable: Core goal of attack is achieved. Side effects may happen (i.e., leak) which other attackers value as low level.
Tier 5	Extremely valuable: The outcomes are highly desired by the attacker(s) and other 3^{rd} parties, with $tier_{3-5}$ rewards.

To assess the reward of a cyber-attack, MaCRA models valuable outcomes based on a five-tier reward value system (see Table II) either as a static value (i.e., one tier) or a range of tier values. The flexibility of value ranges is useful as, for instance, different attackers and secondary effects may be modeled simultaneously. Consider a fishing vessel's activity log stored on a vulnerable on-ship computer. An attacker could gain access to the data on-board and then use the compromised system to target, and attack, other systems as a secondary effect. In the MaCRA framework, this is modeled by a range of values as the secondary effect could increase the possible reward value of the initial attack. Similarly, modeling specific attacker groups (e.g. terrorist factions) or individuals may shift the range of reward upwards or downwards, depending on their characteristics. This is demonstrated fully later in Section IV.

D. Framework Overview

As $axis_{1-3}$ of the MaCRA model have been clearly established, this section provides an overview of the framework. Although MaCRA was introduced as a three dimensional matrix, in actuality it has a much higher dimensionality as all three axes are functions of multiple variables, such as attacker, vulnerability, and mitigation defenses. Specifically, we consider an $attacker$ and a $target$ to have the following attributes when considering maritime cyber-risks:

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

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

Where a_{vector} represents the attack-vector (e.g., vulnerable web application), a_{goal} is the attacker's desired result (e.g., stolen information, physical collision), a_{type} represents the attacker profile as shown in Section II-C, and $a_{resources}$ represents an attacker's access to skill, time, money, members, etc. For the target, $t_{vulnerabilities}$ represents the set of weaknesses (e.g., outdated operating system (OS) or firewall), $t_{effects}$ represents the possible impacts if the vulnerability is exploited (e.g., loss of navigation), t_{type} is the target's type (e.g., oil tanker, fishing vessel, port cargo machinery) and $t_{resources}$ represent experienced crew, updated IBS, anti-virus, etc.

The attributes of both attacker and target are directly related to each other, as an attack vector is directly related to a target's vulnerabilities, and an effect can only be desirable if the target is capable of producing that effect. Furthermore, the types (e.g., tanker, activist) and resources (e.g., insider threat, alert crew, time) of both attacker and target must be considered together to accurately assess risk levels. How MaCRA models $axis_{1-3}$ using these attributes can be seen below, where the attacker can be of any hacker type and the target can be any maritime system,

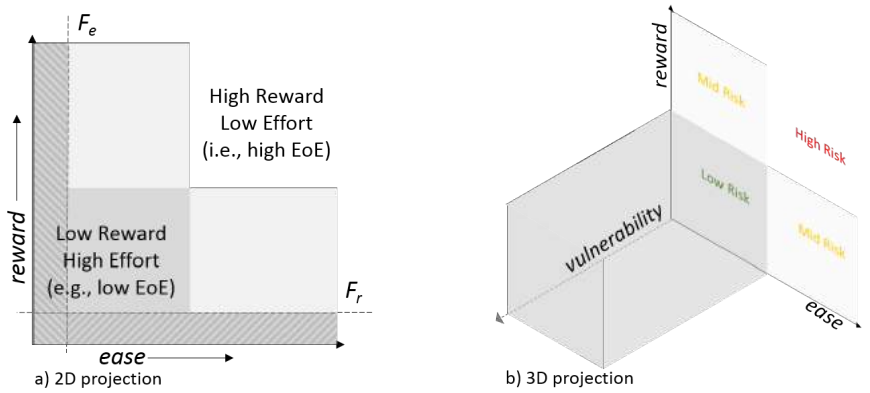


Fig. 1. Projection of MaCRA to risk quadrants for assessing $f_{risk}()$ for systems with reward F_r and effort F_e filters.

vessel, or fleet. More specifically, attributes from Equations (1) and (2) describing $attacker_a$ and $target_t$ are central to the following equations for $axis_1$, $axis_2$, and $axis_3$:

$$axis_1 = f_{vulnerability}(a_{vector}, t_{vulnerabilities}, t_{effects}) \tag{3}$$

$$axis_2 = f_{ease}(a_{type}, t_{type}, a_{resources}, t_{resources}) \tag{4}$$

$$axis_3 = f_{reward}(a_{type}, t_{type}, a_{goal}, t_{effects}) \tag{5}$$

From equations (3) - (5) we use $f_{risk}(attacker, target) = I(f_v(a,t), f_e(a,t), f_r(a,t))$ to plot various graphs and assess both general and specific risks given scenarios of interest. Hence, each individual system vulnerability may be projected onto a plane like in Figure 1 (a) using attacker reward and ease (EoE). A series of these representational graphs, where each system is projected onto a 2D risk quadrant, would allow an assessor to compare the risks of various systems at face value, but also in specific scenarios with a range of factors for consideration. While risk can be evaluated by the data point's distance from the origin (i.e., risk indicator function $I()$), it can also be generalized by the risk quadrant a vulnerability is mapped to.

In Figure 1, the top right quadrant defines the highest risks, as systems projected there have the most reward for the least attacker effort. If an analyst possesses limited resources for threat mitigation, filters F_{effort} and F_{reward} may be introduced to filter out risks related to low-reward or unrealistically high-effort attacks. These could then define acceptable risks and focus security efforts for optimal investment, as cyber defenses can be time and resource consuming. This partially illustrates MaCRA's abilities, with Section IV exploring such projections further.

III. System Vulnerability Evaluation

This section introduces and evaluates popular ship systems, many of which are mandated and regulated by existing governing bodies (e.g., IMO [21], CFR [22]). While not a complete set of the global fleet's systems, as that data does not yet exist (see Section VI), regulations do make the technologies in this section, many of which are unique to the maritime industry, a reliable representational set of realistic modeling data to populate MaCRA with. This is demonstrated in several use-case assessments in Section IV. The following subsections categorize systems into navigation, positioning, communication, and physical asset (i.e., cargo) management. Lastly, it examines the human factor and a few specialized systems. Each category is concluded with a breakdown of the covered systems belonging to that category, with an overall summary of vulnerabilities and impacts shown in Table III and a connected view of systems in Figure 2.

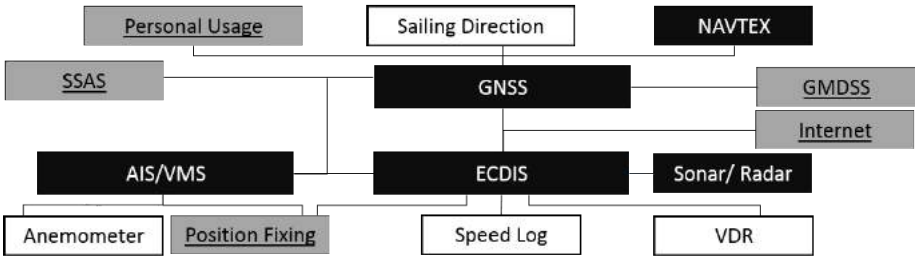


Fig. 2. Integrated Bridge System (IBS), grouped roughly by function (e.g., navigation).

A. Navigation Systems

As navigation is a core function of all maritime ships, and due to mandatory electric charts (i.e. e-charts) [23], navigational system technologies are some of the most significant in the maritime industry and its cyber-vulnerabilities would be of interest to any of the modeled attackers. Thus it is important to consider the effects of plausible cyber-attacks and whether the attacker's aim is to misguide, confuse, deter, or damage. Figure 3 maps these systems to more specific technologies and possible cyber-attack effects in a simplistic projection of `MaCRA` data. For example, the projected view in Figure 3 shows that AIS holds the most technological vulnerabilities and may be used to trigger the most effects, with damage seemingly the most likely impact. This is related to how navigational systems are relied on, and compromised directions may result in collisions.

Electronic Chart Display and Information System (ECDIS) was mandated by the IMO safety committee in 2009 for all vessels engaged in international voyages [23], with very few ships exempted from this. This system is designed to display either electronic navigational charts (ENC) or digital nautical charts (DNC) for navigation and is a central to the modern ship bridge. IMO regulations also have several performance standards and resolutions for electrical charts (e.g., A.817(19), MSC.64(67)) that may increase its attack surface [21]. ECDIS is also highly interconnected with other navigation sensors and water reference systems (e.g., radar, Navtex, AIS, depth sonar) and requires a minimum of weekly ENC updates produced by official providers such as the UK and US hydrographic offices. All three update methods, via Internet/satellite, USB and CD/DVD, present network, hardware, and social engineering vulnerabilities with potentially low `EoE` levels and high rewards for multiple attackers [24]. Further studies have also shown that the underling ECDIS OS (e.g., Windows XP) and its flaws could result in a multitude of attacks including the modification or deletion of ECDIS data [25]. As an amendment to the SOLAS regulation, vessels equipped with ECDIS may use raster chart display systems (RCDS) in case of failure, but many ship outfitters have opted for a second, redundant, ECDIS instead [23], [26].

Automatic Identification System (AIS) was made mandatory for all ships above a gross tonnage on international and non-international voyages by the IMO in 2004 [27]. To prevent collisions, AIS signatures are broadcast by marine radio or satellite (i.e., S-AIS) to provide information about a ship's identity (e.g., name, call sign), navigation status (e.g., at anchor), rate of turn, heading, type, position, course, speed, and the bearing of shore stations, other ships, and aircraft [21]. This data is broadcast at regular time intervals, and a typical ship's class-B-transponder broadcasts its position every five seconds when traveling faster than 23 knots. AIS transponders are comprised of GPS and VHF radio commutation technologies, both of which can be hacked via network and transponder protocol attacks [22], [28]. Furthermore, software implementations of online providers may also be compromised to attack a ship's AIS. Previous research (see Section V) has also revealed numerous vulnerabilities in AIS to allow the modification of ship details, create ghost vessels, false alerts, and modify signal transmission

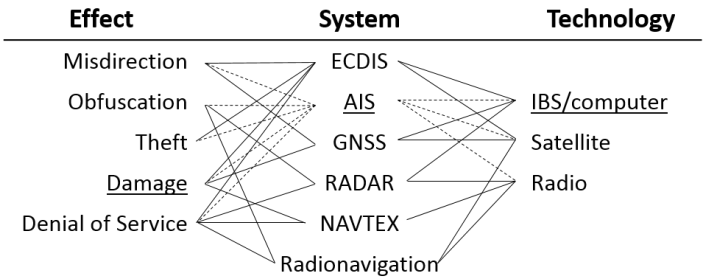


Fig. 3. Mapping of effects and technology of navigation systems.

frequency [17], [29]. In 2014 it was reported that Somali pirates used online AIS data to identify and manipulate victims, as well as counterfeit AIS data to mislead victims or obfuscate their own position [30]. In 2013, a North Korean ship concealing 240 tons of weapons reportedly turned off its AIS to hide its voyage [31]. These are not isolated events, as an Israeli firm recently found that, in one day, 100 ships counterfeited AIS data and transmitted incorrect locations [30]. At the very least, criminal and terrorist attacker types would have an interest in these systems. However, while an attacker may compromise AIS to trigger an effect, trained crews can prevent this from occurring and `MaCRA` is able to model such defenses using the `EoE` axis.

Global Navigation Satellite System (GNSS) is a constellation of satellites that transmit time and positions from orbit. The four satellite networks of note are (1) US Global Positioning System (i.e., GPS or Navigation Satellite Timing and Ranging (NAVSTAR)), (2) Russian Global Navigation Satellite System (GLONASS) (3) Europe's Galileo, and (4) the Chinese BeiDou system. Satellite is used in the maritime industry for global position fixing data and is one of the most interconnected and valued IBS system. Based on its value, GNSS would make a likely target for most attackers. Moreover, its low-energy signals are a significant technological weaknesses as it often experiences interference from natural solar flares, the earth's ionosphere, other radio frequencies, and spectrum congestion. Therefore active interference, like jamming and spoofing [32], [33], [34], could present a high-value, low-effort attack. Due to the interconnected bridge, loss of GPS can also result in the failure of other important systems such as AIS, speed logs, and Global Maritime Distress and Safety System. In 2014, a GPS jamming experiment was performed by the UK and Irish General Lighthouse Authority on the ship Pole Star, which entered jamming zones to study the resulting ship failures and crew reaction [35]. North Korea has also actively used GPS jammers against South Korean to interfere with military and civilians systems at sea and on land, with an estimation of 700 ships affected in the attacks [36].

Radio Detection And Ranging (Radar) detects physical objects by using radio waves to determine range, position, and trajectory [22]. While radar signals are more difficult to jam than the aforementioned satellite, it is still possible with more advanced techniques. Jamming technologies previously developed for submarines and aircraft include mechanical, electrical stealth, and intentional interference. Simplistic interference can occur when two radars are in close proximity and operate on the same frequency. Sophisticated attacks may focus all its jamming power on a single frequency, sweep full power through a range, jam several frequencies at its source, or fake positioning by delaying pulse transmissions [36]. In 2014, the GPS signal of USS Donald Cook, a 4^{th} generation guided missile destroyer, was completely jammed by a Russian aircraft boasting sophisticated radar jamming technology in the Black Sea [33]. While effort required for a denial of service (DoS) attack is relatively low for any attacker, as a ship is equipped with more relied-upon navigation systems, radar-based attacks may yield low-reward.

NAVTEX, i.e. Navigational Telex or narrow-band direct printing (NBDP), was designated by the IMO to provide warnings, urgent marine safety alerts, and both meteorological and navigational forecasts via a radio technology, e.g. SITOR collective B-mode [22], [37]. While regulated receivers must receive international broadcast frequencies at all times, non-regulated receivers can switch. This simplicity and the fact that NAVTEX is not essential in most scenarios means attackers have few methods or reasons for attacking this system. That said, possible jamming attacks or an infected ship PC may prevent NAVTEX signal decoding or allow message tampering [37], [38]. Attacks may be used to delay shipments or cause damage if sent into a storm. As some NAVTEX data is now downloadable via the internet, its EoE may increase. As seen in Figure 3, NAVTEX is one of the least technological advanced navigational systems and is not able to produce as many effects as AIS or ECDIS, but could still result in damage.

Radionavigation was a popular radio-based navigation tool used by many different users before the rise of GNSS [22]. While some of these technologies are obsolete (e.g., Transit and Omega hyperbolic satellites were removed in the 1990's), there has been an effort to bring back the navigation system Loran-C as eLoran, a low frequency, long range navigation system. Primarily redesigned as a complementary fall-back, i.e. an independent satellite system that is harder to jam or spoof, eLoran has seen delays as many see it as a redundant and outdated system [39]. If ever deployed, eLoran would attract similar attackers as the other navigational systems (e.g., GNSS), but possibly less so if it is truly more robust against cyber-attacks.

B. Positioning Systems

Although similar to navigation, positioning systems have been placed in a separate category as these technologies report data on more immediate surroundings, which leads to different effects when compromised. These systems often interface with navigation, as the data derived from them are useful for guidance. For example, a loss in GPS signal could significantly affect position fixing, although approximate positioning can be made solely based on ship sensors. This, however, can lead to in-accurate positioning. According to one incident report, the Royal Majesty ship grounded itself due to a disconnected GPS antenna cable. Because of this, the ship's autopilot was therefore unable to take into account the effects of wind, current, and sea conditions, which eventually resulted in a 17-mile discrepancy in positioning [40]. As the outcomes of attacking sensors for position fixing can be unpredictable, it is more likely an attacker will invest the effort into exploiting navigational systems. However, increasing navigation system security may shift attacker attention to position fixing for similar outcomes. Figure 4 summarizes the maritime positioning systems discussed at the end of this subsection, by mapping each system, its core technologies, and possible effects. To make it more visually comprehensible, the most common item of each column is underlined and connected with dotted lines.

Sailing Directions published by the National Geospatial-Intelligence Agency (NGA) provide planning and en-route guides for ship crews. It interfaces with navigation systems like ECDIS and contains time zones, coastlines, ports, harbors, firing areas, search and rescue information [41]. In one of the worst oil spills in history attributed to inaccurate sailing directions, the bulk carrier Sanko Harvest was grounded on an Australian reef causing massive amounts of damage due to out-dated sailing direction information. More recently, it was reported that in 2013 a vessel sailing through Chinese waters damaged a fish cultivation area because it was not marked on the ship's charts. This was due to missing local chart data which had not been uploaded and on-route updates were disabled due to a non-functioning NAVTEX system [42]. Extrapolating from these incidences, malicious activities could cause ships to enter or avoid certain zones, which can be valued by any of the cyber-attacker profiles given the possibilities.

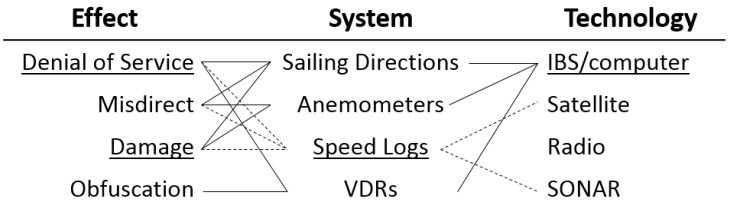


Fig. 4. Effects and technologies of positioning and propulsion systems.

Speed Logs can be generated by echo-sounders, like Sound Navigation and Ranging (**SONAR**) devices, GPS measurements, or propeller rotations and pitch. Speed from propellers may be calculated from the main vessel propeller's rotations per minute (RPMs) or by a small propeller mounted to the hull. Of these speed-measuring technologies, GPS and sonar have the most cyber-attack vectors. The vulnerabilities, cost, and rewards of attacking GPS have already been discussed. Tampering with the sonar system, which is more useful for detecting objects under the water for positioning, might have little consequences as ships often have redundant sonar systems to avoid obstacles. However unlikely, unreliable sonar readings have resulted in collision incidences. For example, two nuclear submarines collided in 2009 within the Atlantic Ocean, as their anti-sonar devices prevented both vessels from detecting each other [43].

Anemometers measure wind speed. Its accuracy depends on the shape and structure of a ship, as the hull and superstructures (e.g., towers and cranes) could result in airflow distortions, leading to biased wind speed measurements. The World Meteorological Organization (WMO) Voluntary Observing Ship (VOS) program recruits thousands of merchant ships to report meteorological conditions on the ocean's surface and then, after accounting for any bias as mentioned previously, produce detailed weather forecasts. The system itself is not likely to be of high interest to an attacker due to its low impact. However, from a cyber-security point of view, if it is possible to gain control of higher-valued systems on the same network, its reward value as a target would increase from an attacker's perspective. While crossing the Atlantic Ocean, a large passenger ship was once affected by the loss of its anemometer. Furthermore, one of the radar scanners was damaged and stopped working. While the lack of wind speed measurements made travel more difficult, the trained crew was able to take the vessel to safety with an eight hour delay [44].

VDRs, i.e. voyage data recorders, have been made mandatory by the IMO for all passenger ships and all other ships over 3,000 GRT (gross register tonnage) to assist in accident investigations. VDR's constantly record and store the date, time, ship position, speed, heading, bridge audio, communication audio, radar, AIS, depth, main alarms, wind speed, direction, and anything else that an investigator may find useful. This is analogous to the "Black Box" known for airplane incidences. While the data itself is unlikely to be stolen, as a secondary attack any possible evidence may be altered or wiped to protect the attackers. In 2015, it was reported that an Indian cargo ship's VDR data files were overwritten and lost using a USB stick [45]. This resulted in the loss of data for a 12 hour period, during which the vessel had collided with a fishing trawler. Analysis of the system showed weak encryption, insecure authentication, a flawed firmware update mechanism, and various services plagued by buffer overflows and command injection vulnerabilities. Due to the VDR's design, it is most likely to be attacked physically by an insider, and less likely for a sophisticated attacker to attack remotely, which `MaCRA` can model with differing `EoE` and reward factors.

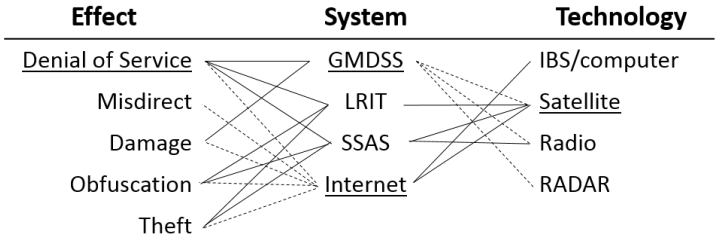


Fig. 5. Mapping of effects and technologies of communication systems.

C. Communication and Networking Systems

This section examines three forms of communication, those meant for humans, machines, and human-machine interactions. A summary of these systems can be found in Figure 5, which demonstrate how, due to the nature of communication, the likeliest attack on these systems will have a denial of service effect (DoS) to prevent communications such as distress calls.

Global maritime distress and safety system (GMDSS) is a collection of automated emergency communication equipment and protocols considered as one of the basic global requirements for ocean-going ships [46]. The main system components of a GMDSS are (1) emergency position-indicating radio beacon (EPIRB), (2) NAVTEX to distribute maritime safety information (MSI), (3) Inmarsat global mobile services overseen by the international mobile satellite organization (IMSO), (4) high-frequency radiotelephone and narrow-band radiotelex for communication, (5) search and rescue transponders based on radar (SART) for distress signals, and (6) digital selective calling (DSC). Thus GMDSS requires a range of radio frequencies for ship-to-ship distress alerts, search and rescue coordination, on-scene communication, maritime safety information, and bridge-to-bridge connections [22]. Preventing communications, e.g. as a secondary DoS attack, could isolate a target and disrupt rescue attempts and GMDSS is particularly vulnerable to malicious firmware which, if installed, can allow an attacker to control devices on-board the vessel and deliver false data by spoofing and disrupting signals [47].

Ship Security Alert System (SSAS) was created to strengthen maritime security with covert transmissions of satellite (Inmarsat D+) and radio alerts to local authorities [22]. More specifically, SSAS beacons were designed to suppress acts of terrorism, piracy, and mutiny, therefore being denied communication is a concern. SSAS is not currently required to be integrated with the more generic, encompassing GMDSS, but they can be combined in order to contact law-enforcement. Conversely, dedicated SSAS modules are available if integration is undesirable.

Internet access on ships is provided via the shipboard network, which has a gateway to the global internet. This in turn provides local networks for personal usage and to connect ship systems. Typically, ship workstations connected to the internet will be running older versions of Microsoft Windows (e.g., XP), although some may run Linux, both of which are common on-shore OSs with well-researched network-based attack surfaces [48]. Furthermore, the average age of the global fleet (i.e., 20.3 years [2]) and long voyages have lead to outdated systems and large windows of opportunities, where an attack can occur after a vulnerability is discovered but before the ship can be updated. For example, email is an attack vector where dangerous software can be downloaded, or the user can be guided to vulnerable websites. If the on-board network system has weak encryption algorithms or insecure protocols (e.g., hard-coded credentials), remote attackers may easily take remove control of critical ship systems via any internet connection [47].

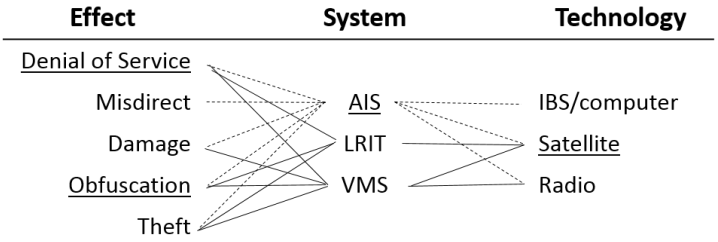


Fig. 6. Mapping of effects and technologies of identification systems.

Long-ranged identification and tracking (LRIT) provides global ship identity data, similar to AIS, and ship tracking. Ships are obligated to transmit LRIT data, due to IMO regulations [49]. When compared to AIS, LRIT has more global coverage as it only uses satellite and utilizes a more secure end-to-end data transfer. Compromising LRIT cannot misdirect ships the way a compromised AIS can, but as it is key for search and rescue services when upgraded with GMDSS Inmarsat C, DoS is the most concerning and plausible attack on this system.

As ship networks are often not segregated and insecure, a single attack could affect multiple systems [48]. For example, one compromised personal device could weaken the overall IBS security, and so it is important to consider all systems from a security perspective, despite how trivial a system may seem from a maritime perspective. Lastly, as bandwidth capabilities increase, ship systems like NAVTEX are increasing their internet dependencies to obtain data, entertain guest and crew, and interact with foreign systems. As this interconnectivity trend continues, the reward value of an attack dramatically increases, while EoE may stay relatively static.

D. Identification and Information Systems

Several of the systems discussed in the previous sections also serve as identification broadcasters. For example, frequent AIS broadcasts which are designed for collision avoidance also include the vessel's maritime mobile service identity (MMSI), IMO ship identification number, name, radio call sign, type and dimension of ship, and destination [27]. Similarly, LRIT also transmits vessel name, IMO number, and MMSI identification. However, in comparison to AIS broadcasts, LRIT transmission data is more secure from 3^{rd} parties. It has been speculated that pirates have used ship ID data to target and monitor specific ships. To mitigate this relatively new behavior, regulations have been altered so ships can legally switch off their AIS to avoid such situations [50]. Lastly, AIS allows on-shore authorities to identify vessels within a nation's exclusive economic zone. If AIS information can be turned off or altered, attackers can obfuscate their activities to avoid detection during repeated crimes or those with a long duration.

Vessel monitoring systems (VMS) can be considered as the fishing equivalent of the more generic AIS. However, VMS is only mandatory for a small percentage of fishing vessels, as the vast majority are less than 24 meters and thus exempt [51]. VMS uses automatic location communications (ALC), the most widely accepted of which is an Inmarsat-C transceiver with built-in GPS. Primarily satellite-based, as opposed to AIS's mostly VHF-based radio, this closed proprietary service is a ship-to-shore communicator which is more suited for fishing routes as they tend to follow coastlines more closely than other vessel types (e.g., transoceanic container ships). VMS transmits essentially the same data as AIS (e.g., location, identification numbers) and VMS protocols have been similarly altered in the past to obfuscate illegal activities [28], [52], but the cyber-risks are slightly different as only large fishing vessels would be affected.

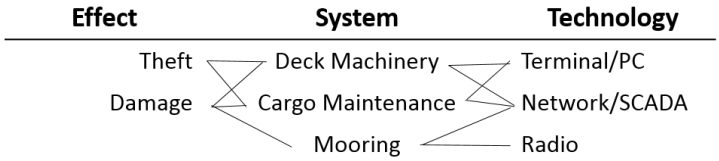


Fig. 7. Mapping of effects and technologies of cargo and machinery systems.

E. Cargo and Machinery Management Systems

Including both digital on-ship systems and ship-to-port interfaces, cargo and machinery management systems are vulnerable when access is unrestricted, identifications are checked incorrectly or infrequently, and when access points are not physically protected. Summarized below are several basic deck and cargo machinery types. Currently, port-based systems are not considered, although MaCRA can be extended to encompass its entirety in future work (see Section VII). Although more simplistic than the previous MaCRA $axis_1$ mappings of maritime systems to technical vulnerabilities and possible outcomes, Figure 7 maps the discussed cargo and machinery management systems. This may change drastically as technology, e.g. remote control, evolves.

General cargo deck machinery are pump and motor systems used to power deck winches, cranes, derricks, and windlasses. This machinery performs the heavy lifting regarding cargo and ship equipment, but may perform other functions such as anchoring. The exploit pay-off of these systems would nominally be destroying or stealing cargo, but may include physical damage to the ship, nearby entities, or the environment. Direct attacks are currently unlikely given the limited attack surface, and it is more likely that the IBS or engineering controls would be attacked to control these systems, e.g. via supervisory controls and SCADA networks. A recent rise of cyber-attacks on similar SCADA systems, like water treatment plants, highlight significant vulnerabilities in the system despite where it has been applied [53], [54]. As machinery become more intelligent, remote-controlled or automated [12], direct attacks may increase.

Mooring ships has evolved from manual labor to automated systems, which were developed to improve physical safety and efficiency [55]. Although automated systems may enable ports to make infrastructure savings, an attacker may achieve the opposite if a ship were to collide with onshore structures or cause congestion. This can be achieved today, as modern mooring technology can be remotely control via radio [55], [56]. This results in several networking vulnerabilities such as DoS via radio jamming [56], power cut [55], and packet replay. The latter occurs when a previous, legitimate, command is recorded and played back to perform the action once again. Similar techniques have been used previously for car-jacking [57].

F. The Human Factor and Specialized Systems

Although systems are becoming more sophisticated, even automated, humans still account for a large part of a working ship. Studies estimate that 75%-96% of maritime casualties are caused, at least in part, by human error [10]. While this has traditionally pertained to machinery-based accidents [6], it is becoming more prevalent in the cyber sector. Training and awareness exercises are needed to prevent social-engineering based attacks as well as prepare, and better equip, crew and on-shore teams to quickly detect, deter, or mitigate cyber-attacks. The human factor is therefore an important aspect to consider for both public and private sectors, as manipulating a person via cyber-attacks can be equally devastating as attacking a technological system in terms of economic loss, reputation loss, and physical damage. While malware can be used to compromise devices, blackmail and phishing emails can be used to compromise people.

Insider threats are a critical aspect of cyber-security as they often have access to information that reduce the effort required to launch certain attacks (i.e., increase EoE). Cyber-vulnerabilities may be triggered intentionally or accidentally, with only the former considered as a cyber-attack in this paper. Insider threats may be caused by a disgruntled or malicious employee, a compromised (e.g., blackmailed) insider, or a malicious attacker who acquired legitimate access via legal or illegal means. Disgruntled insider threats [16] may often act as activists, if they have an idealistic goal like whistle-blowing, or criminals, if they are interested in financial gain. For mariners, an increase in disgruntled crew members has partially resulted in members staging pirate attacks on their own ships [19]. There has been similar increases in exploitation, with blackmailed employees both on-shore and at sea [20], [58]. As ships and crew physically move and connect to a wide range of local and foreign networks, a higher chance of insecure network connections increase significantly when compared to other stationary systems. Lastly, as a subset of extortion, sextortion is a growing concern and the U.S. Navy has seen an increase in reported instances with victims having paid in excess of $11,000 to perpetrators [59], [60].

As an example of accidental insider threats, social media such as Facebook have been reportedly used as an intelligence source for criminals in the Gulf of Aden [17]. In one case, although a ship passenger uploaded detailed images of vessel safety measures to their Facebook account, the crew were aware of the possible consequences and altered the ship's course before entering the gulf. As demonstrated by this example, awareness levels of how systems and information should be protected can greatly help or hinder a ship in the event of a maritime cyber-attack, which is why $target_{resources}$ is an important factor modeled by MaCRA to assess risk.

Apart from the human factor there are a few more specialized systems the authors wished to address. This is an incomplete list, as ships can be highly specialized and modified, but includes some notable technologies for maritime-cyber risk assessments. Access to the **inert gas system**, which is used to prevent explosions on oil tankers, could have a significant incentives for certain attackers. As the operator terminals for these systems are available via either MODBUS or Ethernet, network-based attacks are feasible [61]. Similar scenarios include protection and maintenance systems (e.g., **cooling, heating, ballast**), which are essential for ship, crew, and cargo safety. Such systems are still primarily mechanism-based, but can be controlled through a computer terminal, e.g. in engineering. Pentesting (see Section VI) is likely needed to determine specific vulnerabilities. Another system worth mentioning is monitoring. There has been a recent increase in demands for **CCTV** like camera solutions on-board ships. As a common technology on-shore, it is an established system with known vulnerabilities [62], [63]. This may be more useful for covering up internal crimes, but may be used with external physical attacks.

The **integrated bridge system** (IBS) was introduced as a collection of technologies, however the IBS itself must be viewed as a single system. There are several products available today provided by companies like Raytheon, eGlobe, Kongsberg, ECPINS, Sperry, JRC and Transas. Apart from the construction, e.g. how systems are connected, policies on system interactions are essential, as the combined systems result in a complex sets of possible configurations and actions. For example, how the IBS should to react if GPS signal is lost would determine important policy, as displaying incorrect data may be more detrimental than disabling the screen. Similarly, alert and warning systems should be designed to support crews, otherwise high priority alarms may be ignored or missed [64]. Maliciously triggering or silencing alarms could also drastically distract and stress crew at critical moments to increase the probability of incidences or as low-level attacks. Future work, as described in Section VI, shall also include the engine room, as that is a second hub of concentrated technology within a ship that an attacker would be highly motivated to compromise. This is particularly important as the systems evolve away from mechanical-based.

TABLE III
SYSTEM VULNERABILITIES AND EFFECTS

Cyber Vulnerabilities	System	Physical/Cyber Effect(s)
[USB, SCADA]	Deck Machinery	[damage, theft]
[radio, power]	Auto-Mooring	[DoS, damage]
[USB*, satellite, Internet, IBS]	ECDIS	[DoS, damage, mis*, theft]
[VHF, satellite, radar, IBS]	AIS	[DoS, damage, mis*, theft, obfu*]
[satellite]	GNSS	[damage, mis*]
[radar]	Radar	[DoS, o]
[USB*, satellite, Internet]	IBS/Main PC	[DoS, damage, mis*, theft, obfu*]
[USB*, Internet, NBDP, IBS]	NAVTEX	[DoS, damage]
[radio, LORAN]	Radionav	[DoS, damage]
[radio, satellite, ECDIS, NAVTEX, IBS]	Position Fix	[DoS, damage, mis*]
[SONAR, satellite, propeller]	Speed Logs	[DoS, damage, mis*]
[]	Anemometers	[DoS, m]
[USB*, IBS]	VDR	[DoS, obfu*]
[radio, NAVTEX, satellite, radar]	GMDSS	[DoS, damage]
[satellite, SSAS]	LRIT	[DoS, damage, theft, obfu*]
[radio, NAVTEX, satellite, radar]	SSAS	[DoS, theft, obfu*]
[satellite, USB*, IBS]	Internet	[DoS, damage, mis*, theft, obfu*]
[satellite, LORAN]	VMS	[DoS, damage, theft, obfu*]
[network, IBS]	CCTV	[DoS, obfu*]
[MODBUS, network]	Cargo Maintenance	[damage]

mis* = misdirect, obfu* = obfuscation, *USB =+ CD/DVD

Lastly, it seems important to mention **eAtoNs**. Previously, AIS was mentioned as a ship anti-collision system, while more recently, stationary AIS aids to navigation (AtoN) beacons have been installed on navigational hazards, such as wind farms, oil platforms, bridges, and buoys to provide anti-collision data for stationary objects. More recently, virtual electronic AtoNs (i.e., eAtoNs) have also been introduced for environments where physical AtoNs are impossible or problematic to anchor. This includes identifying coral reefs and defining Arctic shipping passages where ice movements present a challenge [65]. While not yet a widespread practice, as these virtual objects exist firmly within the cyber domain and cannot be visually checked, this could be a high-risk target for attackers seeking collision and misdirection incidences.

IV. MaCRA RISK ASSESSMENT EXAMPLES

From the data gathered on technological systems, attacker profiles, and possible outcomes in Sections II and III, MaCRA can be sufficiently populated for several demonstrative risk assessments. The set of discussed system vulnerabilities and their potential effects has also been collated into Table III, excluding specialized systems from Section III-F and those outside the scope of this study. From Table III, $axis_1$ of MaCRA would map two points for the VDR system as it has two possible cyber-attack effects, `(VDR : DoS)` and `(VDR : obfuscation)`, four points for ECDIS, and three for SSAS. Within this study, the full set of effects considered in this paper are `damage`, `theft`, `denial of service`, `misdirect`, and `obfuscate`. As the MaCRA dataset develops and grows with realistic shipping data, more effect types or subtypes may need be considered (see Section VI) to maintain detailed and useful risk assessments. For the full 3D model, $axis_1$ maps the full set of maritime system vulnerabilities and their possible effects, as shown in Table III. $Axis_2$ and $axis_3$ are modeled using the defined activist, competitor, criminal, and terrorist hacker types. Details of target and attacker attributes are varied and discussed within each scenario, and are specifically chosen to create interesting scenarios for MaCRA to assess. Once the basic projected views and filters of MaCRA have been demonstrated in Sections IV-A – IV-D, a more detailed scenario with more realistic attacker and ship data is used in Section IV-E to fully discuss MaCRA's risk assessment abilities in detail.

The following scenario-based assessments have been designed to show-case MaCRA's ability to model, discover, and assess maritime cyber-security risks. As the first four of the examples only extract a small number of systems, attackers, and targets, the resulting assessments may seem simplistic, as they only utilize the data needed for specific assessments. Future work and details (e.g., directly from shipping companies) would be required for a complete risk-assessment model of the global fleet, however, based on current regulations, the vast majority of maritime ships are equipped with the systems detailed in Table III [23], [27], [49]. Thus, the following examples could be considered relevant as real-world assessments, and any lack of detail does not prevent this study from demonstrating how MaCRA can be used to view and assess maritime-cyber risk. Moreover, MaCRA is still functional despite vague or missing details by substituting ranges for fixed values when defining $attacker$ and $target$ attributes (see Section II-D). This allows an analyst to perform realistic assessments with moderate levels of data.

A. Yacht Scenario: Hactivist vs Criminal

In this scenario, the target is an expensive yacht. The wealth of $target_y$'s passengers makes them, and their data, of interest to criminals, i.e $attacker_c$. In addition, local hacktivists, $attacker_h$, are concerned about $target_y$'s increased boating activity in a delicate marine ecosystem. While $target_y$ is equipped with some network-defenses, the ship has an unusually large number of custom network-based systems (e.g., personal entertainment), which introduces more cyber-vulnerabilities than the average ship. To compare the risks of $attacker_c$ and $attacker_h$ on $target_y$, this data can be modeled and extrapolated into Figure 8. The view presented in this visualization shows that the top risks to $target_y$ are information theft by $attacker_h$ via the main bridge computing system, followed by misdirection and theft, physical and intellectual, by $attacker_c$ via ECDIS or AIS. Furthermore, $target_y$'s highest risk is information theft via the ISB, as both activists and criminals would find it a low-cost, high-reward outcome.

This projection of underlying model data onto a contextualized two-dimensional plane can help risk assessors quickly conclude that criminals and ecosystem-activists would not be interested in causing physical damage to this target with a cyber-attack, and such attacks may be considered a low-risk event despite the fear factor. In this scenario, Figure 8 also demonstrates how MaCRA can model ranges for attacker attributes instead of fixed values. This is useful, as the model can adapt to different subsets of $attacker_{type}$ and $attacker_{resource}$ levels. It then also becomes possible for organizations such as insurers to see the risks associated with the worst case scenarios (e.g., the largest hactivist organizations) as well as the best case scenarios. In this projection, as activists tend to be smaller organizations (i.e., attacker $tier_{1-3}$), horizontal dotted lines can be used to extend EoE into higher tiers to show that this group is likely to have less resources to spend on an attack, decreasing ease. Conversely, criminal types range widely (i.e., attacker $tier_{1-5}$) and so the dotted lines are distributed more evenly across the "ease" axis. As can be seen, this shifts the risk of $attacker_c$ into a higher risk zone than $attacker_h$. The last factor to consider regarding resources is their impact on the outcome, as shown by the dotted line's length. For example, jamming technology ultimately works independently of the user's skill, and would therefore have a shorter line than more skill-dependent cyber-attacks, like data theft.

Figure 8 also demonstrates how MaCRA can instantly shift data within projected views as variables change in real-time. For instance, if $attacker_h$ lost resources in a police raid their EoE would raise. Similarly, if $target_y$ missed an important AIS security patch, the risk profile would change again. MaCRA is capable of modeling these changes to the appropriate variables, as demonstrated by the arrows in Figure 8, whether adapting to real-time changes, or while deciding which security solutions to apply in order to optimally and effectively decrease risk.

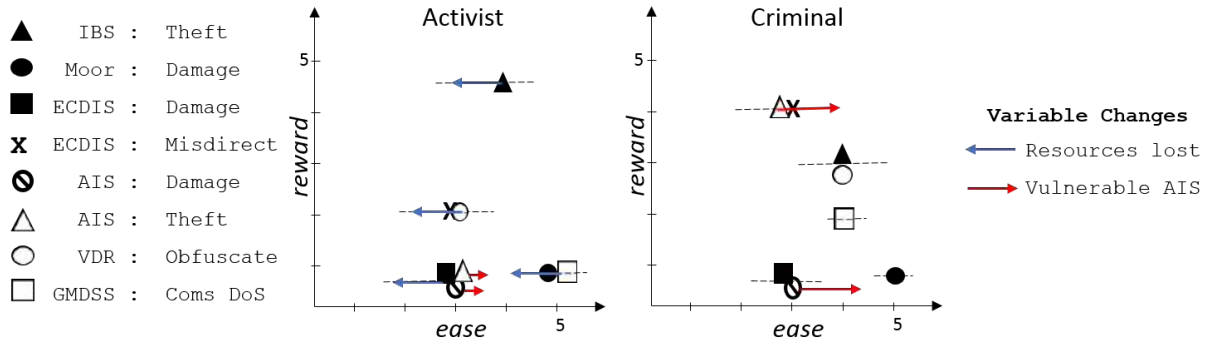


Fig. 8. Changes of a yacht's risk considering range of activist and criminal attackers with ranged EoE.

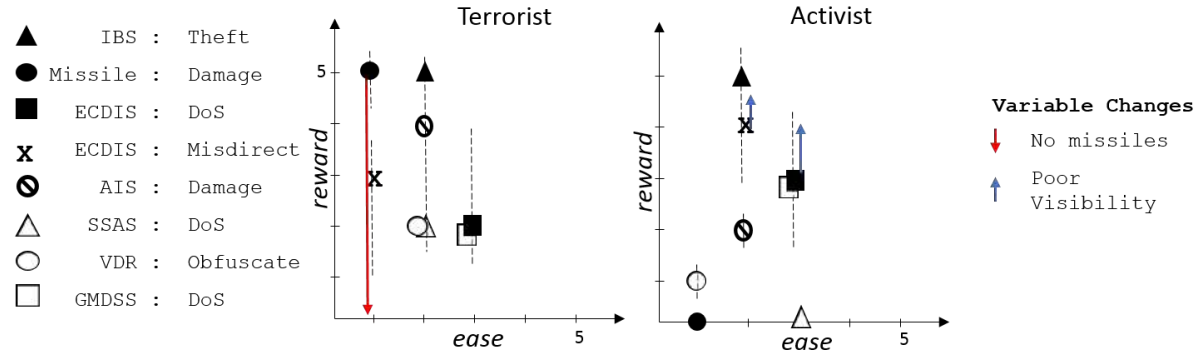


Fig. 9. Changes of a Naval vessel's risk considering Terrorist and Activist attackers with ranged reward.

B. Military Scenario: Terrorist vs Hacktivist

From an examination of possible scenarios, the cyber-attackers that seem to put navy ships at the most risk are terrorists and hactivists (i.e., $attacker_t$, $attacker_h$). It seems less likely for a native competitor attacker to target their own nation's naval fleet, and an external competitor committing cyber-attacks would likely be considered more of a criminal, or even a terrorist. Furthermore, it seems unlikely for a criminal hacker to target the military unless they have terrorist tendencies or connections to such organizations. In this scenario, military $target_n$ is equipped with a state-of-the-art anti-jamming GPS for its missile guidance, but lesser radio-based communications can be jammed or spoofed. Furthermore, the underlying bridge OS is outdated which, despite additional military hardening, has several vulnerabilities. The goal of $attacker_h$ is to protest military decisions and delay operations, whereas $attacker_t$ is interested in intelligence information and possibly in compromising $target_n$'s missile weapon system.

From this scenario model, shown in Figure 9, the top risk based on the risk quadrants is information theft, since both modeled attackers would be interested in the data and, even if neither valued it, a third party would be due the powerful and covert nature of military information. Furthermore, the vulnerable OS in this scenario increases the attack `EoE`. In comparison, while $attacker_t$ may be equally, or more, interested in compromising the weapon system, it is much better protected and very difficult to compromise, which is also apparent when compared to Figure 8. Lastly, as each type of attacker contains sub-sets or sub-types (e.g., terrorist factions), Figure 9 demonstrates the range of goals and resources based on `MaCRA`'s variable $attacker_{goal}$

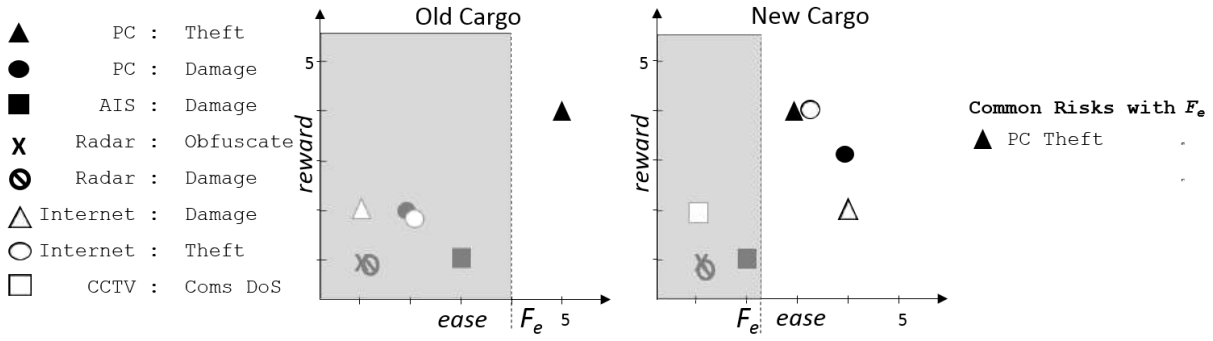


Fig. 10. Common filtered risks of a competitor attack on both old and new cargo ships.

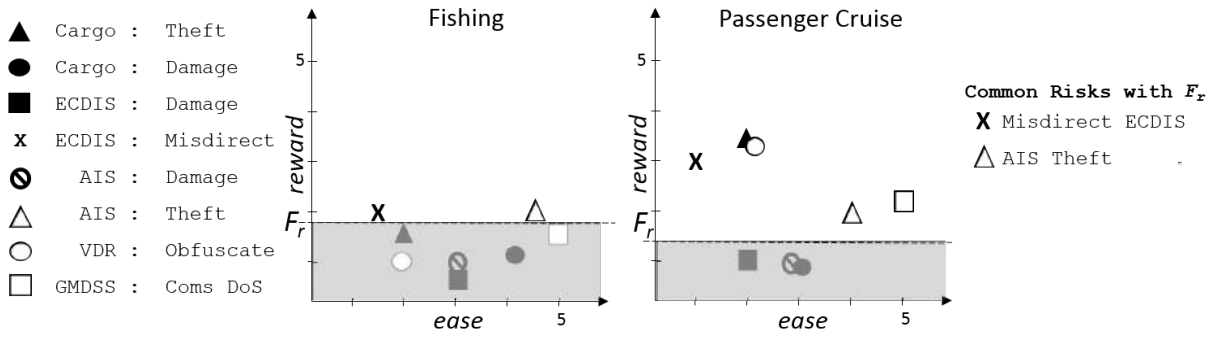


Fig. 11. Common filtered risks of a fishing vessel and cruise ship considering a criminal attacker.

and $attacker_{resources}$ attributes using vertical dotted lines. The range of interest tends to be wide in niche outcomes, as they may be very valuable or not at all for different attackers.

While it is possible to show additional shifts in risks based on variables that changes EoE (see Figure 8), in this assessment the authors shall demonstrate the MaCRA framework's ability to reflect risk changes on the reward axis due the target's change. Specifically, Figure 9 demonstrates the change in risk if $target_n$ were to offload its missiles at a base or if the target were to venture in a region of low visibility, as a loss in navigation would suit $attacker_h$'s goal of delaying naval operations. This is to demonstrate subsets of MaCRA's abilities while, in reality and later scenarios, the effect of relevant attribute changes are much more elaborate and may impact both $reward$ and EoE differently for various systems or attackers at different levels.

C. Competitor Scenario: New vs Old Cargo Ships

In this scenario, the projected views shown in Figure 10 are to help assess the risks of a competing shipping company, $attacker_c$, deploying cyber-attacks against another company's cargo ships. In this specific scenario one of these ships is 30 years old and the other is brand new, i.e. $target_o$ and $target_n$ respectively. This scenario aims to illustrate how MaCRA can model and project views that highlight subtle, yet essential, target differences when considering risks, as the ships in this scenario perform the same cargo-shipping functionality, but still have different risk profiles due to their attributes. While individual systems on $target_o$ may have more vulnerabilities, air gaps prevent some attacks and basic systems using low bandwidth may decrease both EoE and reward for a cyber-attacker. Conversely, the newer ship is updated but

untested, therefore it is unclear if the systems are configured correctly or will behave as expected. Moreover, its complexities and interconnectivity may increase its attack surface. Within this scenario, $attacker_c$ represents saboteurs on both target ships with the primary goal of stealing data, such as manifests and shipping data. This differs slightly from normal criminal activity, for while some may attempt to steal and sell data to competitors etc., the majority are more likely to target physical goods at ports rather than attack them at sea. A second $attacker_c$ objective is to stealthily damage the target's reputation by introducing operational delays and altering data to mishandle shipments. If a target has limited resources, MaCRA can be use for optimal investing.

Another tool MaCRA provides for real-world assessments, is the ability to define acceptable and not-acceptable risks since security solutions can be costly and not every risk can be reduced to zero. Section II-D first introduced ease and reward filters (i.e., F_e, F_r) for this purpose, and in this scenario, the targeted company has chosen to invest most of its resources to protect the newer $target_n$ against cyber-attacks. Therefore, as shown by the filtered gray areas in Figure 10, F_e classifies more acceptable risks on the $target_o$ than $target_n$. As F_e filters based on attacker effort, sophisticated attacks are determined as acceptable risks under the assumption that they are unlikely to happen based on the average attacker's skill and other resources. As the filters in Figure 10 show, an assessor may view common non-acceptable risks for $attacker_c$. In this case, data theft is a risk to both ships, and so the targeted company should make improving data protection its first priority as it would result in a significant drop in risk for both of its cargo container ships. The non-acceptable risks in this scenario all happen to be high-mid risks as well, based on the reward factors. However, if some of these risks also had a low reward value, they may also be classified as acceptable risks, as demonstrated in the following scenario.

D. Criminal Scenario: Fishing vs Cruise Ship

In this scenario, MaCRA is used to model one criminal $attacker_c$ and two targets (i.e. fishing vessel $target_f$ and cruise ship $target_c$) and assess the relevant risks. While the international passenger cruise $target_c$ has more security built into the ship than a $target_f$, it is not sophisticated enough to prevent advanced attacks (i.e., $tiers_{3-5}$), although on-board alarm systems may still detect a cyber-intrusion and trigger the proper warnings and alarms. Conversely, there is vastly less security on $target_f$ which may make both intellectual and physical theft easier. However, the fishing vessel's route never takes it too far from shore, and so the response time of authorities is much shorter unless a DoS attack is launched. Several projected views for aiding assessments can be found within Figure 11, demonstrating the use of MaCRA's reward filter (i.e., F_r). The purpose of this filter is to separate risks associated with low-reward attacks, despite the EoE. Such risks within this particular scenario are then disregarded solely based on the assumption that the outcomes are not worth $attacker_c$'s effort, including any secondary outcomes.

Within this scenario, the company that owns $target_c$ has delegated slightly more resources for ship cyber-defenses than the fishing company has for $target_f$. This is illustrated by the placement of the F_e filters within Figure 11. The differently sized risk quadrants defined by these filters determine different sets of acceptable risks and highlight non-acceptable risks based on $attacker_c$'s most desired goals. For $target_f$, the assessment determines its main risks are AIS-based theft and ECDIS misdirection. These two are also ranked high for passenger ships. In addition, this scenario's $target_c$ is at-risk to GMDSS denial of service, VDR obfuscation, and kidnapping (i.e., cargo theft) due to the non-trivial rewards for $attacker_c$. More realistically, an assessment would use both F_e and F_r filters to classify ECDIS misdirection for fishing and kidnapping for cruises as acceptable risks, as the $attacker_{effort}$ seems extreme, but for demonstration purposes this and the previous example only utilize one filter each.

TABLE IV
A MORE REALISTIC RISK MODEL FOR TWO OIL TANKERS

	Tanker A: **Route 1**								Tanker B: *Route 2*							
	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	1	3-4.5	1-2	3-4.5	3-5	4-5	3-4	**4-5**	1	3-4.5	1-2	3-4.5	3-5	4-5	3-4	**3-4**
AIS : Misdirect	3-4	3-4.5	1-2	3-4.5	3-5	3-5	2-4	3-5	3-4	3-4.5	1-2	3-4.5	3-5	3-5	2-4	3-5
AIS : Theft	1	3-4.5	1	3-4.5	3-5	2-5	2-3	2-5	1	3-4.5	1	3-4.5	3-5	2-5	2-3	2-5
Cargo : Damage	0	3-4	0	**2-5**	0	4-5	0	4-5	1-2	3-4	1	**4-5**	1-2	4-5	3-5	4-5
Cargo : Theft	0	4	0	**2-5**	0	4-5	0	4-5	1-2	4	2-3	**4-5**	3-5	4-5	3-5	4-5
CCTV : DoS	2	3	1-2	**1-2**	1-2	3-4	1-2	3-4	2	3	1-2	**2-4**	1-2	3-4	1-2	3-4
ECDIS : Damage	1	2	2-3	**3-4**	2	2-3	3-5	**2-3**	1	3	2-3	**4-5**	2	3-4	3-5	**1-3**
ECDIS : DoS	2-4	1-2	2-4	**1-4**	2-3	2-4	2-4	**2-4**	2-4	1-2	2-4	**3-4**	2-3	3-4	2-4	**1-4**
ECDIS : Misdirect	3-5	2-3	2-4	**2-4**	2-4	2-4	2-5	**2-4**	3-5	3-4	2-4	**4-5**	2-4	4-5	2-5	**1-4**
GMDSS : DoS	1-2	***1-2***	1-2	***1-2***	1-2	***1-2***	1-2	***1-2***	1-2	***1***	1-2	***1***	1-2	***1***	1-2	***1***
Internet : Damage	2-5	2-4	3-5	2-4	1-2	2-4	3-5	**3-4**	2-5	4-5	3-5	4-5	1-2	4-5	3-5	**4-5**
Internet : Theft	3-5	1-4	3-5	1-4	3-5	1-4	3-5	**2-4**	3-5	2-4	3-5	2-4	3-5	2-4	3-5	**2-4**
Moor : DoS	1-3	3-4	1-3	***1***	1-2	3-4	1-2	3-4	1-3	3-4	1-3	***1-2***	1-2	3-4	1-2	3-4
PC/IBS : Damage	2-5	3-5	3-5	4-5	1-2	4-5	3-5	4-5	2-5	3-4	2-5	3-4	1-2	3-5	3-5	4-5
PC/IBS : Theft	3-5	3-5	3-5	2-4	3-5	3-5	2-5	3-5	3-5	1-3	3-5	1-3	3-5	2-5	2-5	3-5
Radar : Damage	1	***4-5***	1	***4-5***	1	**3-4**	3-5	***2-3***	1	***2-4***	1	***2-4***	1	**2-3**	3-5	***3-4***
Radar : Obfuscate	1-2	3	1-2	3	1-2	**3-4**	2-5	***2-3***	1-2	3	1-2	3	1-2	**2-3**	2-5	***3-4***
SSAS : DoS	1	***3***	1	***3***	2	***3***	2	***3***	1	***2***	1	***2***	2	***2***	2	***2***
VDR : Obfuscate	1-2	4	1-2	**3-4**	2-5	4	2-5	4	1-2	4	1-2	**4**	2-5	4	2-5	4

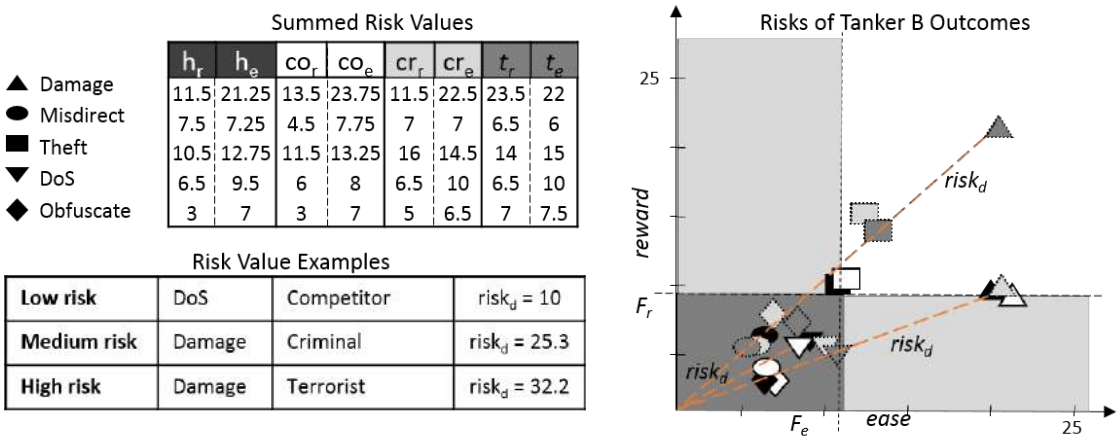
Abbreviations	
h	Hactivist
co	Competitor
cr	Criminal
t	Terrorist
r	Reward
e	Ease-of-Effort

Tanker Details	
A	no cargo, better IBS/network protections, route passes pirate area and shored ports
B	has cargo, upgraded ECDIS, route passes terrorist area and tight channels

E. Other Views: Realistic Tanker Scenario

As the MaCRA framework models a wealth of information in a multi-dimensional space, there are many ways to extract the data to assess specific scenarios, as seen in the previous examples. However, a multitude of risk assessments other than the ones shown in Figures 8-11 are possible by extracting different data sets. For the remainder of this section, MaCRA risk assessments will be made based on the more realistic data modeled in Table IV. While previous examples selected a small subset of attackers, ships, and systems to illustrate certain MaCRA abilities, all attacker profiles and systems discussed in this article have been modeled. As MaCRA is currently unable to model the entire global fleet, Table IV models oil tankers $target_A$ and $target_B$ including in-depth details of the ships and their voyages. Typographic differences illustrate how different attributes have effected the values of $axis_{1-3}$ within the model. Additional columns can be added later to extend the model to encompass additional ships or new attacker profiles, and more rows may be added if more `(system : effect)` pairs are introduced or discovered.

In this scenario, $target_A$ carries a secure IBS system and on-board computer. It is sailing without cargo on $route_1$, which includes ports shared with other shipping companies, and enters a moderate hot-zone for pirate activity. The second oil tanker $target_B$ is carrying cargo, but does not have the same security upgrades as $target_A$. However, $target_B$'s ECDIS in isolation is more secure than $target_A$'s ECDIS is isolation. Lastly, $target_B$'s route passes a terrorist zone and physically narrow channels that may make land-based denial of service attacks more feasible. From this data MaCRA can, for example, use both F_e and F_r filters together to identify several sets of risk. Such sets may be categorized into low-, medium-, and high-risks, or acceptable and non-acceptable risks. For example, consider Figure 12 and the four risk quadrants (i.e., $risk_q$) divided by the filters F_e and F_r. Low risks equate to the darkest bottom-left quadrant, medium equates to the two light gray quadrants, and the set of high-risks in the top right quadrant are not highlighted. Similarly, on the same figure, the three gray quadrants may be considered acceptable risks whereas the top right quadrant would remain as non-acceptable risks. If no filters are present, $risk_q$ may be defined by halving the highest EoE and reward values.



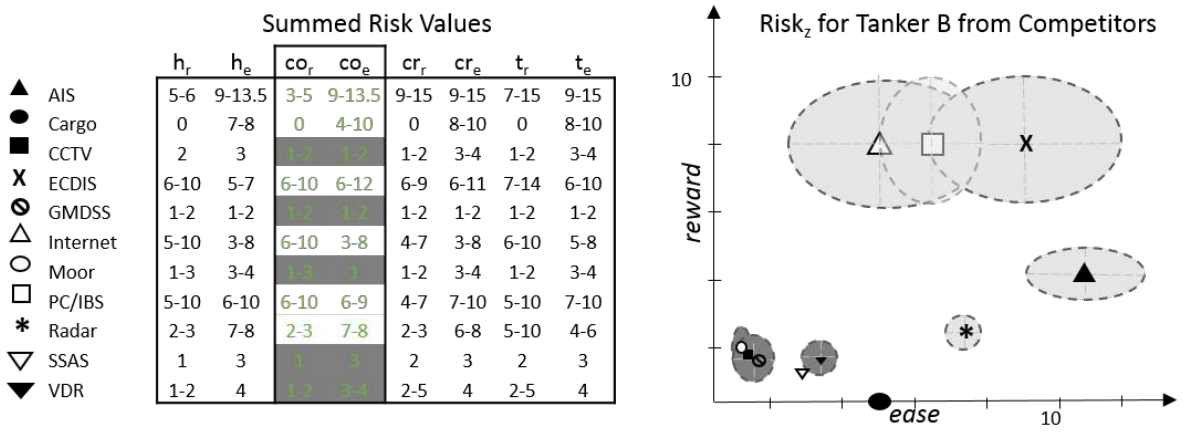
h_r	h_e	co_r	co_e	cr_r	cr_e	t_r	t_e
11.5	21.25	13.5	23.75	11.5	22.5	23.5	22
7.5	7.25	4.5	7.75	7	7	6.5	6
10.5	12.75	11.5	13.25	16	14.5	14	15
6.5	9.5	6	8	6.5	10	6.5	10
3	7	3	7	5	6.5	7	7.5

Fig. 12. Averaged summed effect risks of Tanker B with risk quadrants defined by filters.

Similarly, the risk of each `(system : effect)` pair on $axis_1$ may be quantified by calculating its distance (i.e., $risk_d$) to the origin using risk indicator $I()$ as it was presented in Section II. The may be done in isolation, or to rank risks within defined sets (i.e., $risk_q$). The latter is recommended, as calculating $risk_d$ alone could result in misleading assessments. For example, although the $risk_d$ values may be equivalent, a military target would most likely rank a low-EoE risk higher than high-EoE risk, as they must be prepared for highly-sophisticated adversaries. When considering the highest risks of $target_B$ in Figure 12 after applying the filters F_e and F_r, terrorist damage ranks highest with a $risk_d$ of 32.2, followed by criminal and terrorist theft, $risk_d$ of 21.59 and 20.52 respectively. As this tanker's route passes through a known terrorist zone that $target_A$ does not (see Table IV), this is as expected. The other high risks may also be the result of an IBS that is more vulnerable than the one in $target_B$.

The reason that the table values of Figure 12 exceed the normal 1-5 tiers as defined by the MaCRA framework, and shown in Table IV, is that each row is the summation of all similar effects despite the system that caused this effect. As each value in MaCRA's risk assessment model is defined with the system and effect, one can also assess the total risk of one system through the summation of reward and EoE values to create a new point or zone. As the summation method may be applied to fixed values or variable ranges, this can create risk zones, i.e., $risk_z$, for further consideration. Risk zones, as shown by Figure 13, may be useful when considering ranges of attacker attributes and target resources, as it may be impossible to identify all relevant factors at the time of assessment.Figure 13 sums the risk of each system in Table IV so that each row represents a system's risk, despite the attack effect. This summation pushes technologies with multiple vulnerabilities further into the high-risk quadrant. For an assessor wishing to determine which system upgrade would reduce risks most, this is a useful extrapolation of model data. While Figures 12 and 13 reduce matrix rows, applying the summation method to targets or attackers can reduce the model columns to determine risks disregarding $attacker_{type}$ or individual targets. In summation, the three MaCRA methods for measuring or displaying risk discussed have been:

- $Risk_d$: Calculates risk with indicator function $I()$ as defined in Section II-D as the *distance* from the origin point or area of risk (see Figure 12). A higher $risk_d$ equates to more risk;
- $Risk_z$: Risk *zones*, e.g. Figure 13, use variable ranges to view multiple scenarios at once;
- $Risk_q$: The projected view's planes are divided into *quadrants*, equal sized or filter defined (e.g., Figure 12), to label risks as low, medium, high, acceptable, or non-acceptable.



	h_r	h_e	co_r	co_e	cr_r	cr_e	t_r	t_e
AIS	5-6	9-13.5	3-5	9-13.5	9-15	9-15	7-15	9-15
Cargo	0	7-8	0	4-10	0	8-10	0	8-10
CCTV	2	3	1-2	1-2	1-2	3-4	1-2	3-4
ECDIS	6-10	5-7	6-10	6-12	6-9	6-11	7-14	6-10
GMDSS	1-2	1-2	1-2	1-2	1-2	1-2	1-2	1-2
Internet	5-10	3-8	6-10	3-8	4-7	3-8	6-10	5-8
Moor	1-3	3-4	1-3	1	1-2	3-4	1-2	3-4
PC/IBS	5-10	6-10	6-10	6-9	4-7	7-10	5-10	7-10
Radar	2-3	7-8	2-3	7-8	2-3	6-8	5-10	4-6
SSAS	1	3	1	3	2	3	2	3
VDR	1-2	4	1-2	3-4	2-5	4	2-5	4

Fig. 13. Summed competitor risk zones ($risk_z$) for Tanker A.

While MaCRA is intended to be considered as three dimensional, and all our examples so far have plotted $axis_{1-3}$, dimensions can be reduced for other assessments by considering only two axes or even just one, as each axis in actuality reflects a series of variables as shown in equations (3) - (5). These projected views are useful for a range of assessments, and demonstrate how MaCRA data can filtered and displayed to provide insight on various maritime cyber-risk related aspects. For example, by disregarding the attacker, i.e. only project values of $axis_1$ components, one can visualize the most vulnerable technological systems and what effects those can cause. This view has already been demonstrated in Figures 3-7 and could, for example, enable a company to identify and improve the most vulnerable system(s), or identify all systems that could result in one undesired effect. This is essential for furthering cyber-security and physical-security research for maritime systems as MaCRA risk assessments would ideally highlight the most at-risk systems either individually or globally once it is fully propagated (see Section VI).

The last possible projected MaCRA views the authors wish to discuss concerns the definition of attacker and target, i.e. equations (1) and (2) respectively. In essence, instead of defining a target as one physical system, ship, or set of ships, MaCRA has the ability to consider systems from several ships or structures when assessing risk for one loosely-defined target. This is ideal for modeling systems with frequent interactions, such as ship-to-port interfacing or attackers that work together intentionally or unintentionally. For example, if a ship requires services from a tug boat or land-based cargo crane, the relevant subsystems may be considered in the threat matrix with the original ship as one target, instead of modeling all entities as individual targets. This functionality, demonstrated in Figure 14, can model risks in frequent system interaction, and in the future we aim to further develop this ability for more varied, detailed risk assessments.

The purpose of this section was to demonstrate how the MaCRA model is capable of holding all risk-relevant data for maritime cyber-security, and how a number of assessment views can be produced to compare known risks and discover new, previously unconsidered, risks. The ability to model attacker and target attributes, including relevant semantics, makes MaCRA a powerful risk assessment tool in a quickly developing maritime-cyber landscape for reliably identifying acceptable and non-acceptable risks with quantified values. Assessors are also be provided with model data to determine which systems are high-risk and why (e.g., what impact they can cause) and what types of attackers are most likely to be interested in attacking those targets.

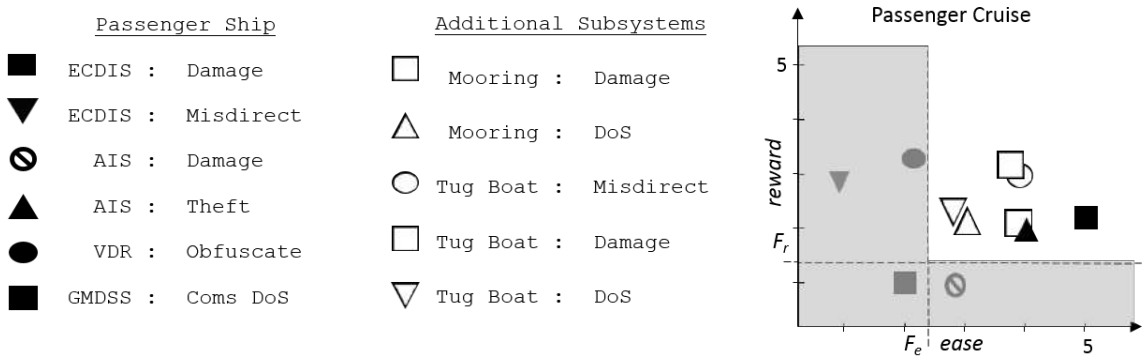


Fig. 14. Risk of ship systems and relevant subsystems of other vessels.

V. Related Work and Limitations

The focus of this article is not on predicting incident risks (e.g., human or machinery-based) based on statistics [66], [67], [68], but is a model-based framework for assessing maritime-cyber risks. The aim of MaCRA is also not to assess the flaws or risks of a specific system, as several previous studies have already found various, isolated, technical vulnerabilities. Researchers have previously found that it is possible to jam or spoof GNSS, modify ship details, create ghost vessels, trigger false alerts, and modify signal transmission frequencies based on focused analyses [17], [28], [29], [30], [31], [34], [69], [70]. Conversely, the purpose of this study is to enable an analyst to determine all risks of maritime-related systems without excluding any technology that may seem unimportant, such as mooring equipment, but may actually pose a large risk when considering all attacker and target attributes. Based on the current research on this topic, the authors felt that more effort in assessing what the major maritime-cyber security risks are will help focus technical solution-based research efforts into areas that require attention as maritime systems grown and attackers find new weaknesses and rewards for their exploits.

To the best of our knowledge, studies focused on individual systems, particularly navigation, represent the bulk of today's maritime-cyber research. For example, incorrect or corrupted digital charts within the ECDIS navigation system have been linked to the groundings of the USS Guardian, CLS Thames, OVIT and other vessels [30], [71], [72], [73]. Additional studies have shown that navigational systems, and VDR data recorders, can be intentionally exploited using software-based cyber-attacks via the Internet, USB, CD, and DVD [25], [41], [45]. Several of these studies overlap with other areas of concern, such as navigation in airplanes or cars [74], [75], [76], [77], and the SCADA systems of smart grids and rails [54], [78], [79]. However, just as risk assessments for aeronautical and land-based vehicles differ due to variations in system designs and environment, any evolving cyber-risk model for maritime must also adapt to its unique factors. While several past maritime-based studies consider risk, they only analyze it for one particular factor [80], as opposed to evaluating an entire ship or fleet, as MaCRA aims to do. For example, other papers have focused on attacker assessments [81], [82] or assessing specific geographical regions where cyber-crimes are prevalent and growing [83], [84].

Other specialized risk assessment methods, frameworks, and standards have long been used for companies, technologies, traffic, management (e.g., ISO), heath care (e.g., SEISMED), safety, and more [85], [86], [87], [88], [89]. In our understanding, there is no well established maritime risk assessment framework covering cyber, and so the MaCRA model would be the first specialized cyber-risk assessment tool for any and all maritime systems, ships, and fleets. However, it is

possible to interface established methods with MaCRA, to enhance its assessments. For example, MaCRA can incorporate more detailed insider-threat models [90], [91]. Like some previous tools, e.g. CORAS [87], MaCRA assessments primarily present data visually, as seen in Section IV. Studies have found this a more intuitive and effective way to evaluate risks [92], [93], which is why MaCRA provides risk zones and quadrants (i.e., $risk_z$ and $risk_q$). However, quantified values are also available as risk measurements (i.e., $risk_d$). Thus MaCRA is able to produce results for for different users, e.g. operators, insurers, and mariners, seeking different assessments.

Currently MaCRA is unable to determine accurate cyber-maritime risks for accidents, including accidentally lowered EoE or increased reward, and while the model data can be altered after the incident, it cannot be modeled beforehand. This includes situations where an attacker accidentally discovers a weakness, or acquires seemingly low-value data that is later revealed to have a significantly higher value. Another limitation in this study is the amount of available data on maritime systems, which shall be addressed in future work. From what the authors can determine, this is the first paper to propose a framework designed to determine the level maritime-cyber risks, from single systems to multiple ships. It is similar but unlike research for automotive and aeronautical, as MaCRA accounts for relevant mobility, environmental and legislative factors in the maritime space, as described in Section II, and considers the entire ecosystem unlike research focused on singular technical systems. This approach can be used complementary to existing maritime risk assessments, as discussed in the following section, but is unique in its ability to identify risks and project useful views for maritime cyber-risk assessments.

VI. Future Work

This article analyzed the maritime sector and, to better understand cyber-threats of the global fleet, developed a comprehensive framework for assessing risk, and illustrated its use with scenarios and projected views. In the future, the proposed maritime cyber-risk assessment model (i.e. MaCRA) will be suitably populated for real-world usage. There are many vulnerable systems in the maritime sector and while they have primarily resulted in accidents, these vulnerabilities may be intentional exploited in cyber-attacks. This paper has enumerated a large set of such vulnerabilities and outcomes in Sections III and IV. Unfortunately, a complete list of maritime systems and their cyber-vulnerabilities does not yet exist. Additional collaboration with the maritime community will be needed to obtain a fuller set of real-world data to enhance the MaCRA model. Future work can then model existing vessels and fleets to understand the full use-cases and abilities in global situations. To increase the framework's usability, future software-based tools shall be developed based on the MaCRA model for more widespread usage. Once a better understanding of the current state of maritime-cyber is achieved, i.e. what are the significant maritime cyber-risks, future work shall develop more fine-grained risks assessments for specialized areas and better security tools and policies. Furthermore, necessary amendments will be made to maritime training and policies to improve awareness and cyber-defenses.

As there are overlaps with other risk assessment models for attackers, SCADA, and more, as MaCRA is developed into software it may useful to interface it with previously defined risk models. This may be particularly useful in areas not effected by differences in the maritime environment and economy. For example models on attacker profiles or hacker mentality [90], [91], [94] may be integrated if they prove to be detailed enough to define maritime-specific attackers such as pirates using purely cyber-based attacks or hybrid cyber-physical attacks. Similarly, previous work on modeling cyber-risks for SCADA, which as previously mentioned is used in smart grids, water plants etc., and satellite, which is used for mobiles and many other systems for communication, may also be adaptable or integrable with the MaCRA model.

Further developments to the MaCRA framework and a more complete set of real-world data will help determine both common and high-level risks in the maritime sector. These risks and their associated vulnerabilities can then be addressed in future research. This may measurably lower cyber-risks for a significant percentage of ships within the global fleet, or measurably lower one entity's risk by mitigating its most significant, high-level risk. Ideally, further research will also anticipate future systems, particularly pertaining to automated ships [11], [95] and ports [12], including analysis of traditionally on-shore systems being adapted to ships, and specialized maritime systems. The internet of things (IoT) will also play a large part in the future of shipping. It is intended that over hundreds of million shipping containers and ships will be a part of the IoT [2], and if it were to be fully achieved, they will represent a large portion of such connected devices. Thus it is essential to consider the risks of future developments.

VII. Conclusions

In conclusion, it is the intention of this article that the proposed maritime cyber-risk assessment (MaCRA) framework be useful for companies, organizations, and individuals to identify and assess relevant risks given any possible maritime-cyber risk scenario, i.e. any combination of ship, system, environment, and attacker, in the unique maritime context. More importantly, by fully populating the proposed MaCRA model with real-world data and creating an array of customizable views, one can discover risks that were not previously considered as the technology of maritime systems evolve and as attackers find new vulnerabilities and incentives for exploring such systems. This is not currently feasible when only assessing one attacker or system at a time, which a lot of maritime-cyber research has been devoted to so far. Moreover, similar cyber-risk assessment frameworks are not fully adaptable to the unique maritime environment. The MaCRA framework was therefore developed in order to provide accurate and quantifiable risk assessments, enabling the maritime community to identify their significant maritime-cyber risks with enough details to help strategically lower those risks and continuously improve the global fleet's cyber-security, i.e. understand the trade-offs of applying or developing security solutions to optimally mitigate identified risks. Understanding these assessments and trade-offs will ideally provide significant cost savings on cyber protection investment, and enable more accurate assessments for maritime cyber-risk insurers, policy makers, and security researchers by constructing different projections of the same underlying data to contextualize the risk in a way appropriate to the multiplicity of target audiences in this sector.

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

[5] USMRC Maritime Cyber Assurance Research, "The reality of shipboard cyber vulnerabilities," USMRC Maritime Cyber Assurance Team (MCAT), 2016.

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

[7] Maersk, "A. P. Moller Maersk improves underlying profit and grows revenue in first half of the year," *Maersk*, Aug 2017. [Online]. Available: https://edit.maersk.com/en/the-maersk-group/press-room/press-release-archive/2017/8/a-p-moller-maersk-interim-report-q2-2017

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

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

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

[11] Rolls Royce, "Autonomous ships: The next step," Marine Ship Intelligence, 2017.

[12] J. Zhang and P. Ioannou, "Automated container transport system between inland port and terminals," ACM Transactions on Modeling and Computer Simulation, 2006.

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

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

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

[16] BIMCO, CLIA, ICS, INTERCARGO, and INTERTANKO, "The guidelines on cyber security onboard ships version 2.0," International Chamber of Shipping: ICS, 2016.

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

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

[19] MarEx, "Nigerian navy: Crewmembers involved in pirate attacks," The Maritime Executive, 2016.

[20] European Cybercrime center, "The internet organised crime threat assessment (iOCTA)," European Police Office, 2014.

[21] IMO Navigation, http://www.imo.org/en/OurWork/Safety/Navigation/, accessed: 2017-05-17.

[22] 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.

[23] I. M. Organization, "Solas chapter V regulation 19: Carriage requirements for shipborne navigational systems and equipment," IMO, 2009.

[24] GPS World staff, "US coast guard issues gps jamming alert," GPS World, 2016.

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

[26] ECDIS Info, "ECDIS Regulations," http://www.ecdis-info.com/ecdis_regulations.html, 2014.

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

[28] M. Balduzzi, "AIS exposed understanding vulnerabilities & attacks 2.0," BlackHat, 2014.

[29] 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.

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

[31] Latin America & Caribbean, "Seized n korean ship: Cuban weapons on board," BBC, 2014.

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

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

[34] 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.

[35] A. Grant, P. Williams, and S. Basker, "GPS jamming and the impact on maritime navigation," The General Lighthouse Authorities, 2014.

[36] National PNT Advisory Board, "Jamming the global positioning system: A national security threat recent events and potential cures," General Lighthouse Authorities, 2010.

[37] Offshore Blue, "A re-cap of the navtex system," Navigator's Newsletter, 2016.

[38] R. Santamarta, "A wake-up call for satcom security," IOActive, 2014.

[39] E. Collier, "eLoran: More accurate & less vulnerable but not a done deal yet," *Marine electronics*, 2017.

[40] A. Degani, *Taming HAL: Designing Interfaces Beyond 2001*. Springer, 2004.

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

[42] Offshore Blue, "Tales of the unexpected," The Navigator: Inspiring professionalism in marine navigators, 2013.

[43] BBC News, "Nuclear subs collide in atlantic," BBC, 2009.

[44] Marine Accident Investigation Branch (MAIB), "Safety digest 02/1997," gov.uk, 1997.

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

[46] SeaCert, "Global maritime distress and safety system (GMDSS) radio operator," Maritime NZ, 2016.

[47] R. Santamarta, "Satcom terminals: Hacking by air, sea, and land," 2014.

[48] H. Simon and H. Ray, "A taxonomy of network and computer attacks," *Computers and Security*, 2005.

[49] International Maritime Organization, "Solas chapter V regulation 19-1: Long range identification and tracking of ships," IMO, 2009.

[50] BigOceanData, "AIS and anti-piracy maritime security," BigOceanData, 2016.

[51] E. Franckx, "Fisheries enforcement related legal and institutional issues: national, subregional or regional perspectives. FAO legislative study 71," Development Law Service: Food and Agriculture Organization of the United Nations, 2001.

[52] U. Krner, H. Greidanus, R. Gallagher, M. Sironi, G. Azzalin, F. Littmann, P. Tebaldi, P. Timossi, and D. Shaw, "Report on authentication in fisheries monitoring," Joint Research Centre (JRC), 2009.

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

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

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

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

[57] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," Network and Distributed System Security Symposium, 2011.

[58] ESC Global Security, "Maritime cyber security white paper: Safeguarding data through increased awareness," ESCGS Cyber Security White Papers, 2015.

[59] U.S. Army Criminal Investigation Command, "Cyber sextortion," CPF 0002-17-CID361-9H, 2017.

[60] ——, "Cybersecurity: Sextortion exploitation of u.s. service members," U.S. Army Criminal Investigation Command, 2017.

[61] M. P. Norway, "Inert gas system (IGG)," Maritime Protection AS, 2017.

[62] 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.

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

[64] P. Traub and R. Hudson, "Alarm management strategies on ships bridges and railway control rooms, a comparison of approaches and solutions," Paper read at RINA Event, at London, 2007.

[65] A. Weintrit, *Activities in Navigation: Marine Navigation and Safety of Sea Transportation*. Taylor & Francis Group, 2015.

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

[67] 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.

[68] 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.
[69] Trend news agency, "Iran oil tankers said by zanzibar to signal wrong flag," Bloomberg, 2012.
[70] J. Suh, "The failure of the south korean national security state," 2014.
[71] Marine accident investigation branch, "Grounding of CSL THAMES in the Sound of Mull 9 august 2011," Marine accident investigation branch (MAIB), 2012.
[72] ——, "Report on the investigation of the grounding of Ovit in the Dover Strait on 18 september 2013," Marine accident investigation branch (MAIB), 2014.
[73] Y. Vandenborn and R. Bell, "Standard safety special edition - ECDIS assisted grounding," Marine accident investigation branch (MAIB), 2015.
[74] C. A. T. Control, "Cyber security project," www.csfi.us, 2015.
[75] 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.
[76] G. Yeomans, "Autonomous vehicles handing over control: Opportunities and risks for insurance," Lloyd's, 2014.
[77] C. Bordonali, S. Ferraresi, and W. Richter, "Shifting gears in cyber security for connected cars," McKinsey&Company Advanced Industries, 2017.
[78] H. H. Safa, D. M. Souran, M. Ghasempour, and A. Khazaee, "Cyber security of smart grid and scada systems, threats and risks," in *CIRED Workshop 2016*, 2016.
[79] R. Collins, "The state of cybersecurity in the rail industry," White paper, 2017.
[80] R. O. Lane, D. A. Nevell, S. D. Hayward, and T. W. Beaney, "Maritime anomaly detection and threat assessment," 13th International Conference on Information Fusion, 2010.
[81] Danish Defence Intelligence Sevice's Center for Cyber Security (CFCS), "Threat assessment: The cyber threat against the maritime sector," Marine Cyberwatch, 2014.
[82] J. H. Committee and S. Harwood, "Cyber risk," Joint Hull Committee (JHC), 2015.
[83] S. Bateman, "Regional maritime security: threats and risk assessments," University of Wollongong, 2010.
[84] K. L. Nankivell, J. Reeves, and R. P. Pardo, "The indo-asia-pacifics maritime future: A practical assessment of the state of asian seas," Daniel K. Inouye Asia Pacific Center for Security Studies (DKI APCSS) and Kings College London (KCL), 2017.
[85] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for scada systems," *Computers & Security*, vol. 56, 2016.
[86] F. den Braber, I. Hogganvik, M. S. Lund, K. Stølen, and F. Vraalsen, "Model-based security analysis in seven steps — a guided tour to the coras method," *BT Technology Journal*, 2007.
[87] M. S. Lund, B. Solhaug, and K. Stlen, *Model-Driven Risk Analysis: The CORAS Approach*. Springer Publishing Company, Incorporated, 2010.
[88] NIST, "Guide for conducting risk assessments - information security," NIST Special publication 800-30, 2012.
[89] T. Sommestad, M. Ekstedt, and H. Holm, "The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures," *IEEE Systems Journal*, 2013.
[90] D. Cappelli, A. Moore, and R. Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Addison-Wesley, 2012.
[91] CERT Insider Threat Center, "Unintentional insider threats: Social engineering," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep. CMU/SEI-2013-TN-024, 2014.
[92] K. Labunets, F. Paci, F. Massacci, and R. Ruprai, "An experiment on comparing textual vs. visual industrial methods for security risk assessment," in *2014 IEEE 4th International Workshop on Empirical Requirements Engineering (EmpiRE)*, 2014.
[93] T. Stålhane and G. Sindre, "An experimental comparison of system diagrams and textual use cases for the identification of safety hazards," *Int. J. Inf. Syst. Model. Des.*, 2014.
[94] D. Rios Insua, D. Banks, and J. Rios, "Modeling opponents in adversarial risk analysis," *Risk Analysis*, 2016.
[95] K. Tam and K. Jones, "Cyber-risk assessment for autonomous ships," IEEE TCS Cyber Security, 2018.