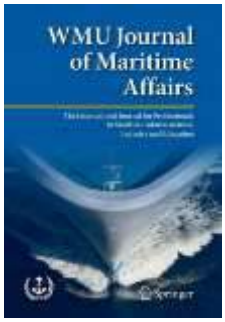


Published as: Kimberly Tam & Kevin D. Jones (2019): MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment, WMU Journal of Maritime Affairs, DOI: 10.1007/s13437-019-00162-2.

Kimberly Tam kimberly.tam@plymouth.ac.uk
Kevin D. Jones kevin.jones@plymouth.ac.uk

WMU Journal of Maritime Affairs (AM) manuscript No.
(will be inserted by the editor)

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

Kimberly Tam[1] • **Kevin Jones**[1]

Accepted: January 7th 2019

Abstract In the current economy roughly 90% of all world trade is transported by the shipping industry, which is now accelerating its technological growth. While the demand on mariners, ship owners, and the encompassing maritime community for digital advances (particularly towards digitization and automation) has led to efficient shipping operations, maritime cyber-security is a pertinent issue of equal importance. As hackers are becoming increasingly aware of cyber-vulnerabilities within the maritime sector, and as existing risk assessment tools do not adequately represent the unique nature of maritime cyber-threats, this article introduces a model-based risk assessment framework which considers a combination of cyber and maritime factors. Confronted with a range of ship functionalities, configurations, users, and environmental factors, this framework aims to comprehensively present maritime cyber-risks and better inform those in the maritime community when making cyber-security decisions. By providing the needed maritime-cyber risk profiles, it becomes possible to support a range of parties, such as operators, regulators, insurers, and mariners, in increasing overall global maritime cyber-security.

Keywords Maritime · Cyber-security · Risk Assessment · Cyber-threats

1 Introduction

Despite the growing number of environmental and economic challenges facing international shipping, the vast majority of global trade, in value and volume, is conducted on the ocean (International Chamber of Shipping 2016a, b). While a significant percentage of the global fleet is devoted to the shipping industry and consists of container vessels, bulk carriers, and tankers, there is still a wide variety of ships designed for pleasure, specialized cargo, military,

[1] University of Plymouth: Maritime Cyber Threats research Group
kimberly.tam@plymouth.ac.uk • kevin.jones@plymouth.ac.uk
https://doi.org/10.1007/s13437-019-00162-2

scientific exploration, and other services (e.g., ice breakers). Due to the significant number of diverse factors involved (e.g., ship type, cargo, route, crew), technologies have been internationally standardized to provide safe and reliable navigation, communication, cargo management, propulsion, and ship-wide monitoring. Standards for these are defined by the International Convention for Safety of Life at Sea (International Maritime Organization (1974)), and are constantly revised as circumstances change (e.g., environmental concerns) and new technology arises. These systems are a novel combination of on-shore and maritime technology, and interconnected in a unique, mobile context, creating interesting cyber-risk scenarios unlike those traditionally seen on-shore.

While increased interconnectivity between ships, personal devices, and on-shore infrastructure has improved operational efficiency and physical safety, it also enables an increase of cyber-attacks, as demonstrated in Allianz Global Corporate and Specialty SE (2016); Jones et al (2016); Maersk (2017) and USMRC Maritime Cyber Assurance Research (2016). While physical security and accident statistics are well understood in the maritime sector, cyber-security is unlike both of these. Normally, a system is considered functioning, or broken. However, with cyber-attacks, a non-functioning system may not be broken (e.g., a hacker can deny system access), and a functioning system may not be trustworthy (e.g., compromised systems can give false data despite seemingly functional). Furthermore, an accident is considered high risk if it is likely to happen, whilst a cyber-attack's risk is based on how easily an adversary can make it happen. Therefore a vulnerability that may be low risk for an accident may have high risk as a potential cyber-attack.

To assess cyber-threats facing ships, crews, and the environment, this paper presents a tool to comprehensively quantify and display maritime cyber-risks. Specifically, in order to be a useful tool for human maritime-cyber awareness and decision making, this framework aims to provide the following:

1. Accurate characterization of maritime-cyber risks and their severity;
2. Scalable measurements from single systems or ships to fleets;
3. Identify systems that would most benefit, or need, additional security;
4. Identify top risk outcomes, attackers, attack-vectors;
5. Provide risk data in useful views to support human decisions.

To accomplish the above, this paper proposes the novel modeling framework `MaCRA` (Maritime Cyber-Risk Assessment) and demonstrates how it comprehensively assesses and conveys risks. For demonstrating plausibility, intentional cyber-attacks are extrapolated from past accidents that occurred due to similar system vulnerabilities. This has significance, as it has been difficult to obtain general statistics on all cyber-related maritime incidents as many of the small-scale attacks currently go unnoticed (e.g., lesser data theft) and some of the more significant attacks have not been released publicly to prevent loss of customers, as mentioned in Allianz Global Corporate and Specialty SE (2016) and Cassidy (2017). It is also likely that the lack of adequate cyber-awareness often results in the misclassification of cyber-attacks as human or machine error (Rothblum (2000); Wingrove (2016)).

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 emergent classes of vessels (e.g., autonomous ships, as seen in Rolls Royce (2017)). While technology changes also increase the number of accidents, see Allianz Global Corporate and Specialty SE (2016), that is not the focus of this article. Instead, this paper examines the maritime risks of intentional cyber-attacks by using a model-based approach that can assess cyber-risks in multiple contexts. The rest of this article is as follows. Section 2 provides an overview of the `MaCRA` framework and how it models maritime cyber-risk variables using attacker and target attributes. Section 3 examines popular ship system technology and analyses them from a cyber perspective for both known and potential cyber-vulnerabilities. Section 4 populates the proposed `MaCRA` model with Section 3 data and exhibits several use-case scenarios and assessments. Section 5 compares `MaCRA` to related works, both in maritime-cyber security and the risk assessment sector, to demonstrate it's unique abilities. And lastly, Sections 6 and 7 conclude with possible research paths for future work and how it can benefit the extensive maritime sector.

2 MaCRA Threat Assessment Framework

Depending on what a person is assessing, different subsets of the underlying data can be extracted from `MaCRA` to create intuitive views. This is important as individuals and organizations will be interested in different aspects of cyber-security. For example, captains, crew, and insurers may all be interested in different aspects of cyber-risk and can view the same risk data in ways that best assist the decisions they make. More specifically, to make the results comprehensible for a wide audience, `MaCRA` is capable of reducing model complexity by projecting risk-assessment views focusing on specific ships, attackers, outcomes, etc. This is a powerful capability for analyzing risk, based not just on one physical ship, but its function and environment, as demonstrated further in the following sections[1]. To this end, `MaCRA` assessments can increase general cyber-risk knowledge and help the maritime community in strategically reducing risks against both known and potential threats.

Based on the well established pattern of general risk and threat assessment models, (e.g., Borgovini et al (1993); Peltier (2005); United States General Accounting Office (1999)), 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) reward. `MaCRA` labels these as $axis_s$, $axis_e$, and $axis_r$ respectively.

[1] All tables and figures were created by the authors to illustrate framework abilities.

2.1 Vulnerability Characteristics

$Axis_s$ of the `MaCRA` framework enumerates a set of system vulnerabilities to be modeled and their possible negative impacts (e.g., `GPS spoofing : ship misdirection`). This provided an interesting perspective as several systems examined may not be important for maritime operations, but could hold significant cyber-vulnerabilities, and it was also clear that maritime systems are not comparative to those in other sectors and should be further analyzed. Figure 1 (b) labels this axis as "vulnerability", as a system can have several.

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, this article gathered sufficient real-world data in Section 3 to showcase the proposed `MaCRA` framework. Although $axis_s$ is primarily based on a ship's on-board technology, it is important to note that environmental factors (e.g., geographic location, weather, crew) are significant variables that are also considered. For example, crew members can be blackmailed or targeted by email phishing attack vectors, as seen in BIMCO et al (2016), and some physical locations provide unique opportunities for attacks like piracy, making `MaCRA` applicable to complex socio-technical scenarios like insider threats and sensitive to global factors like crime, politics, and economics.

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 more and 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. However, a center of sophistical, interconnected systems with a wealth of information and controls is a likely target for cyber attackers. Typical ship systems can be divided by functionality; navigation, control, communication, machinery and cargo management, crew welfare, and specialized, as similarly shown in BIMCO et al (2016). The IBS also often provides an Internet gateway, allowing access to external systems and potentially malicious entities. Section 3 explores these ship system categories further.

2.2 Ease-of-Exploit (EoE)

Semantic, environmental factors play a much more central role in modeling $axis_e$ when determining `EoE`, i.e. how easy a system can be attacked using cyber. For example, the experience and awareness of the crew and passengers could deter or allow a cyber-attack, as seen in CyberKeel (2014a). 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. As another example, if data theft is the attacker's goal, certain ports and networks with weak anti-virus would increase `EoE`.

Table 1 Ease-of-Exploit (`EoE`) with respect to hacker abilities and resources within `MaCRA`.

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 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 more systems targeted at once to achieve goals. Target is well protected with strategic, effective defenses. May not leave forensic evidence, most aspects difficult to detect, and requires significant resources/planning.	Resources include advanced tools, self-made or outsourced, tools to obfuscate attack and bypass defenses.

Unlike $axis_s$, which focuses on modeling the ship systems, $axis_e$ and $axis_r$ determine how likely an attacker is to exploit a cyber-vulnerability to trigger an outcome. 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 1). The tiers descend in number, as `MaCRA` plots the `EoE`. For example, if the GPS on a ship is vulnerable to both jamming and spoofing, and the latter is more complex with a higher "cost" for the attacker, `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 $tier_5$.

Table 1 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 5). Although a limitation in this case, 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.

2.3 Cyber-Attack Reward

$Axis_r$ of the `MaCRA` framework models the end-reward value, as seen from the attacker's perspective. This modeling of hacker incentives determines whether the outcome of an attack is desirable enough to invest the necessary resources. This further differentiates accidents from intentional cyber-crime. To fully understand this aspect of the cyber-attacker psyche, `MaCRA` must correctly model the types of hackers and their motivations. The following closely mirrors traditional cyber-attacker profiles within existing standard security landscape seen in BIMCO et al (2016) and Fitch (2004).

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 context, activists typically want to make environmental, humanitarian, or political-centered 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 as seen in MarEx (2016)), while at the other end there is the increase in organized-crime developing and selling cyber-tools to all types of attackers (i.e., indirect profit), as shown in European Cybercrime center (2014). Lastly, this article considers pranksters as a subset of, mostly low-level, criminals although they may be more "mischief" driven than criminally profit-driven.

Terrorists: While the previous cyber-attackers may occasionally cross a line or cause unintentional, 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 using cyber-tools. In a more sophisticated attack, the ships themselves may become an asset for long distant cyber or physical attacks.

Elitist: In a small niche of today's hacking community, elitists traditionally hacked systems to test, or show-off, their knowledge. Regardless of the decline in such non-profit hackers, this article excludes elitists from the `MaCRA` model because elitist attacks rarely exhibit negative outcomes, as stated in Fitch (2004). However, one could analyze the risks of elitists hackers accidentally causing harm, as they have the capacity for sophisticated cyber-attacks.

Table 2 Levels of cyber-attack rewards as seen by attacker within `MaCRA` framework.

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 2) 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 ship's activity log stored on a vulnerable on-ship computer. An attacker could gain access to the data, although it has little value, and then use the compromised system to target, and attack, other systems which can be more rewarding to say, an activist or competitor. 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 4.

2.4 Framework Overview

As the three axes of the `MaCRA` model have been clearly established, this section provides an overview of the framework. Although `MaCRA` can be viewed as 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, this article considers 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 2.3, 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

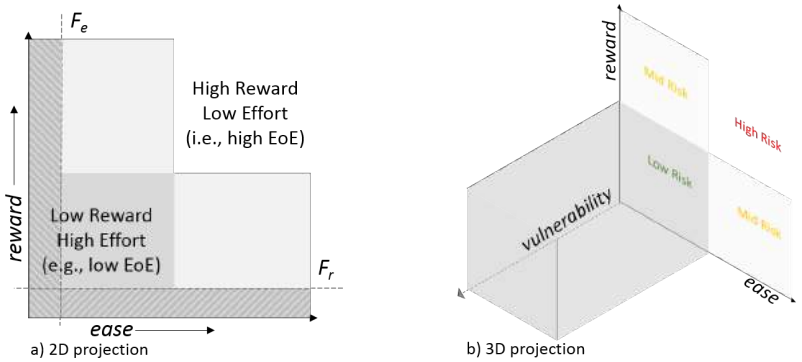


Fig. 1 Projection of `MaCRA` risk quadrants for to assess the $f_{risk}()$ of maritime systems.

type (e.g., river ferry) and $t_{resources}$ represent experienced crew, anti-virus, and other factors that can be used for stopping or catching the attacker.

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 these attributes can be seen below, where the attacker can be of any hacker type and the target can be any maritime system, ship, or fleet. More specifically, attributes from Equations (1) and (2) describing $attacker_a$ and $target_t$ are central to the following equations for $axis_s$, $axis_e$, and $axis_r$:

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

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

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

From equations (3) - (5) `MaCRA` uses $f_{risk}(attacker, target) = I(f_v(a,t), f_e(a,t), f_r(a,t))$ to plot various graphs and assess both general and specific cyber risks given interesting maritime-cyber scenarios. 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

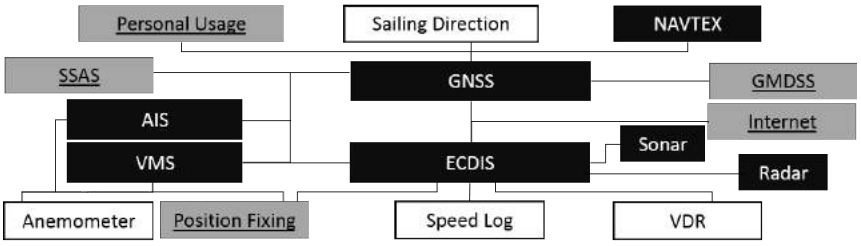


Fig. 2 Integrated Bridge System (IBS), grouped roughly by function (e.g., navigation).

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. Section 4 exploring these `MaCRA` projections further.

3 System Vulnerability Evaluation

This section evaluates popular ship systems with a cyber perspective, many of which are mandated and regulated by existing governing bodies (e.g., IMO Navigation (2017), Archives and Administration (2016)). While not a complete set of the global fleet's systems, as that data does not yet exist (see Section 6), regulations do make the technologies in this section, many of which are unique to the maritime sector, a reliable representational set of realistic modeling data to populate `MaCRA` with. This is demonstrated in several use-case assessments in Section 4. 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 cyber-vulnerabilities and impacts shown in Table 3 and a connected view of systems in Figure 2.

3.1 Navigation Systems

As navigation is a core function of all ships, and due to International Maritime Organization (2009a) mandating electronic charts (i.e. e-charts), navigational system technologies are some of the most significant in the maritime sector 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` $axis_s$ data. For example, the projected view in Figure 3 shows that AIS holds the most cyber-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.

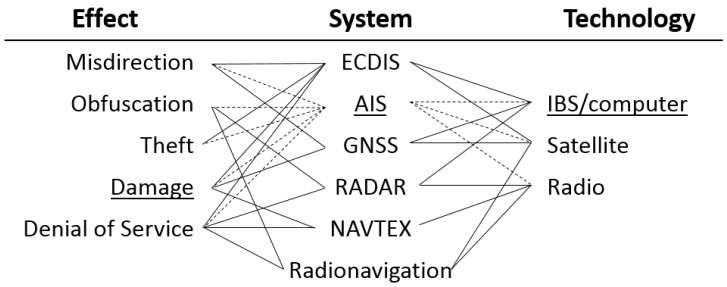


Fig. 3 Mapping of effects and technology of navigation systems within `MaCRA`.

Electronic Chart Display and Information System (ECDIS) was mandated by the IMO safety committee in International Maritime Organization (2009a) and IMO Navigation (2017) (A.817(19), MSC.64(67))) for all vessels engaged in international voyages, with very few ships exempted from this and is designed to display either electronic navigational charts (ENC) or digital nautical charts (DNC). ECDIS is central to a modern ship bridge and is also highly interconnected with other systems (e.g., Navtex, AIS, 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, as shown in GPS World staff (2016). Further studies like CyberKeel (2014b) 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. With International Maritime Organization (2009a) amendments to the SOLAS regulation, vessels equipped with ECDIS may use raster chart display systems (RCDS) in case of failure, but many have opted for a second, redundant, ECDIS instead (ECDIS Info (2014)). While useful for mitigating accidents, redundant systems are less effective in providing robust cyber-security as they may share identical cyber-vulnerabilities.

Automatic Identification System (AIS) was made mandatory for all ships above a gross tonnage on international and non-international voyages, as stated by International Maritime Organization (2004) Annex 17. To prevent collisions, AIS signatures are broadcast by marine radio or satellite, i.e. S-AIS, with ship 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 (IMO Navigation (2017)). This data is broadcast at regular time intervals, and a typical ship's class-A-transponder broadcasts its position every five seconds when traveling faster than 23 knots. AIS transponders are also comprised of GPS and VHF radio commutation technologies, both of which can be hacked via network and transponder protocol attacks as demonstrated in Archives and Administration (2016) and Balduzzi (2014).

Previous research like CyberKeel (2014a) and Mordechai et al (2014) have also revealed numerous vulnerabilities in AIS to allow the modification of ship details, create ghost vessels, false alerts, and modify signal transmission frequency. In Wagstaff (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. In Latin America & Caribbean (2014), a North Korean ship concealing 240 tons of weapons reportedly turned off its AIS to hide its voyage. These are not isolated events, as an Israeli firm recently found that, in one day, 100 ships counterfeited AIS data and transmitted incorrect locations. At the very least, criminal and terrorist attacker types would have an interest in these systems based on their profiles.

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 (GPS), originally known as Navstar GPS, is owned by the US government and run by the US Air Force, (2) Europe's Galileo, (3) the Chinese BeiDou system and (4) Russian Global Navigation Satellite System (GLONASS). Satellite is used in the maritime sector for data like global position and time. It is also one of the most interconnected and valued IBS system. As GPS is connected with all on-board systems, sometimes implicitly, risk may be propagated when location or timing is lost or spoofed. 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, such as jamming (i.e., denial-of-service) and spoofing (e.g., false time or position) (Coffed (2014); Schmidt et al (2016); US Department of Homeland Security (2015)), could present a high-value, low-effort cyber-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 as they rely heavily on timing and location. In Grant et al (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. 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, as stated in National PNT Advisory Board (2010).

Radio Detection And Ranging (Radar) detects physical objects by using radio waves, i.e. microwaves on the electromagnetic spectrum, as shown by federal codes in Archives and Administration (2016). While radar signals are more difficult to jam than satellite, it is still possible with advanced techniques. It is important to note that, while radar and other frequencies on the electromagnetic spectrum (see Tam and Jones (2018b)) are susceptible to noise-based jamming, or more advanced spoofing attacks, the mechanisms to achieve the same effect are significantly different per system. This is due to the various

frequency bands used, signal source, and signal destination. 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. In Coffed (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. 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-value rewards for a hacker.

NAVTEX or Navigational Telex 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 (Archives and Administration (2016); Offshore Blue (2016)). While regulated receivers must receive international broadcast frequencies at all times, non-regulated receivers can switch frequencies. This simplicity and the fact that NAVTEX is not essential in most scenarios means attackers have few methods or reasons for attacking this system. 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. That said, possible jamming attacks or an infected ship PC may prevent NAVTEX signal decoding or allow message tampering, as seen in Offshore Blue (2016) and Santamarta (2014b). Attacks may be used to delay shipments or cause damage if sent into a storm and as some NAVTEX data is now available for download via the internet, its `EoE` may increase.

Radionavigation was a popular radio-based navigation tool before the rise of GNSS, as shown in Archives and Administration (2016). 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, as Collier (2017) claims. 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.

3.2 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 cyber-attacked. 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 this Degani (2004) incident report, the "Royal Majesty" cruise ship grounded itself due to a disconnected GPS antenna cable. Because of this, the ship's autopilot was unable to take into account the effects of wind, current, and sea conditions, and it went into dead reckoning mode which resulted in a 17-mile discrepancy. 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 cyber-security may shift attacker attention. Figure 4 summarizes these positioning systems and maps each to its core technologies and possible effects. To make it more visually comprehensible, common items are underlined.

Sailing Directions published by the National Geospatial-Intelligence Agency (NGA) and the UK Hydrographic Office 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 (Dyryavyy (2014)). In one of the worst oil spills in history attributed to inaccurate sailing directions, the bulk carrier Sanko Harvest grounded on a reef causing massive damage due to out-dated sailing direction information. More recently, Offshore Blue (2013) reported ship 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. Extrapolating from these incidences, intentional attacks could cause ships to enter or avoid certain zones, which could be useful for manipulation, but may not provide enough precision to be useful cyber-attack.

Speed measurements can be made with multiple technologies, even calculated with propeller rotations. For example, in extreme cases Sound Navigation and Ranging (SONAR) devices can send sound waves to fixed objects under the water surface to measure speed. Echo sounding in particular, is a type of SONAR that normally measures depth but can also be used to measure speed using known seabed features. These are relatively safe against cyber-attacks, but not normally used on an average ship (with the primary exception of the military). However, today, GPS measurements are more commonly used for more accurate speed readings. As mentioned previously, the vulnerabilities of GPS mean it has the most cyber-attack vectors of all the speed measuring technologies. The vulnerabilities, cost, and rewards of attacking GPS have already been discussed above. Tampering with the sonar system might have little consequences as any ship with sonar, although rare, would often have redundant systems. That said, however unlikely, unreliable sonar readings have resulted in collision incidences. For example, two nuclear submarines collided within the Atlantic Ocean, as their anti-sonar devices prevented both vessels from detecting each other, as was reported in BBC News (2009).

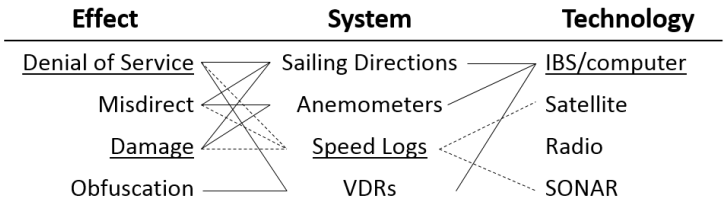


Fig. 4 Effects and technologies of positioning and propulsion system within `MaCRA`.

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. This becomes possible as devices connect to the network or use wireless repeaters. 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, as it was reported in Marine Accident Investigation Branch (MAIB) (1997).

VDRs i.e. voyage data recorders, have been made mandatory by the IMO for all passenger ships and those over 3,000 GRT (gross register tonnage) to help 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 cyber-attack, evidence can be altered or wiped to protect the attackers. In Santamarta (2015), it was reported that an Indian cargo ship's VDR data files were overwritten and lost using a USB stick. This resulted in the loss of data for a 12 hour period, during which the vessel had collided with a fishing trawler. Similar actions could be done intentionally as obstruction. Analysis of VDRs has shown weak encryption, insecure authentication, a flawed firmware update mechanism, and various services plagued by buffer overflows and command injection vulnerabilities. Due to the VDR 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.

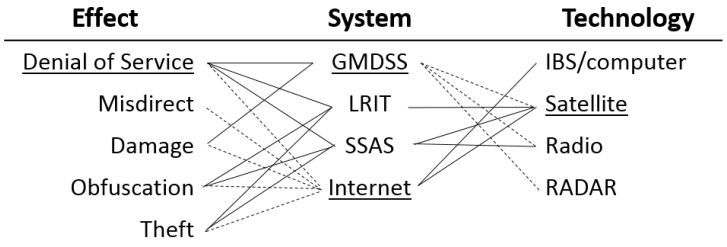


Fig. 5 Mapping of effects and technologies of communication systems.

3.3 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 cyber-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 SeaCert (2016). 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, such as the Cospas System, 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 (Archives and Administration (2016)). Preventing communication can 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 and deliver false data by spoofing and disrupting signals (Santamarta (2014a)).

Ship Security Alert System (SSAS) was created to strengthen maritime security with covert transmissions of satellite (Inmarsat D+) and radio alerts to local authorities (Archives and Administration (2016)). More specifically, SSAS beacons were designed to suppress acts of terrorism, piracy, and mutiny, therefore being denied communication in a cyber-attack is concerning. SSAS is not currently required to be integrated with the more generic GMDSS, but they can be combined in order to contact law-enforcement. Conversely, dedicated SSAS modules are available if integration is undesirable.

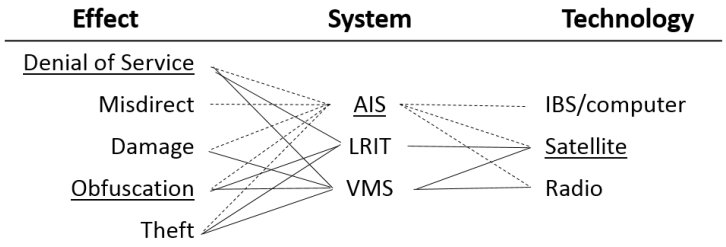


Fig. 6 Mapping of effects and technologies of identification systems in `MaCRA`.

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 onshore OSs with well-researched network-based attack surfaces (Simon and Ray (2005)). Furthermore, the average age of the global fleet (i.e., 20.3 years International Chamber of Shipping (2016)) and long voyages have lead to outdated systems and large windows of opportunities, where an cyber-attack can occur after a vulnerability is discovered but before the ship can be updated. Internet-reliant technology like email is one of the many potential attack-vectors, where dangerous software can be downloaded, or the user can be guided to dangerous websites. Internet-based attacks are already widely used in many sectors, and can be very sophisticated. 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 internet connection, as shown in Santamarta (2014a). As ship networks are not often segregated, and insecure, a single attack could affect multiple systems (Simon and Ray (2005)). 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/crew, and interact with foreign systems. As network interconnectivity increases, and as more network-dependent solutions arise (Costa et al (2018)), the reward value of an attack dramatically increases, while `EoE` may stay relatively static.

Long-ranged identification and tracking (LRIT) provides global ship identity data, similar to AIS, and ship tracking. International Maritime Organization (2009b) SOLAS mandate some ships to carry LRIT, although it is rarer than other mentioned systems, making it less viable for large-scale cyber-attacks. When compared to AIS, LRIT has more global coverage as it only uses satellite and utilizes a more secure end-to-end data transfer, as it is a closed architecture. LRIT protocols are therefore inaccessible, whereas open systems (e.g., AIS) are open to modification and therefore less cyber-secure. 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 cyber-attack on this system.

3.4 Identification and Information Systems

Several of the systems discussed in the previous sections also serve as identification broadcasters. For example, frequent AIS broadcasts must 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, according to International Maritime Organization (2004). 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, practices (see BigOceanData (2016)) have been altered so ships are allowed to switch off their AIS to avoid such situations. 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 (Franckx (2001)). 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 others. 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, as seen in Balduzzi (2014) and Krner et al (2009), but the cyber-risks are slightly different as only large fishing vessels would be affected and operates primarily on a different frequency.

3.5 Cargo and Machinery Management Systems

Including 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. Currently, `MaCRA` does not consider port-based systems, although it can be extended to encompass it in future work (see Section 7). Although more simplistic than the previous `MaCRA` $axis_s$ mappings, Figure 7 shows cargo (e.g., gas) and machinery management systems. This may change drastically as technology, like automation (Zhang and Ioannou (2006)), evolves.

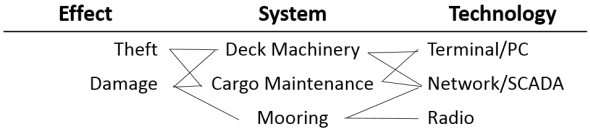


Fig. 7 Mapping of effects and technologies of cargo and machinery systems.

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 cyber-attack surface, and it is more likely that the IBS or engineering, e.g. supervisory controls and SCADA networks, will be targeted to gain access. As an example recent rise of cyber-attacks on similar SCADA systems, like water treatment plants (Igure et al (2006); Leyden (2016)) have shown vulnerabilities that may also apply to similar on-board networks.

Mooring ships is evolving from manual labor to automated systems, which were developed to improve physical safety and efficiency. Although automated mooring help ports this way, a hacker may achieve the opposite effect if a ship were to collide with onshore structures or cause congestion. This could be achieved today, as modern mooring technology can be remotely control via radio (Cavotec (2014); MOOREX (2014)). This results in several networking vulnerabilities such as DoS via radio jamming, power cut, 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, as demonstrated in Francillon et al (2011).

3.6 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 like Rothblum (2000) estimate that 75%-96% of maritime casualties are caused, at least in part, by human error. While this has traditionally pertained to machinery-based accidents (Allianz Global Corporate and Specialty SE (2016)), it is becoming more prevalent in the cyber sector. Training and awareness are needed to prevent social-engineering based attacks as well as prepare, and better equip, crew and on-shore teams to quickly detect, deter, and mitigate cyber-attacks. The human factor is therefore an important aspect to consider, as manipulating a person via cyber-attacks can be equally devastating as attacking a system's technology in terms of economic loss, reputation loss, and physical damage. In summary, while malware can be used to compromise devices, blackmail and phishing emails can be used to compromise people if unprepared.

Insider threats are a critical aspect of cyber-security as they can often access information that reduce the effort required to launch certain attacks (i.e., increase `EoE`). 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, BIMCO et al (2016), may often act as activists, if possessing goals like whistle-blowing, or criminals, if financially motivated. For example, an increase in disgruntled mariners has resulted in at least one staged pirate attack (MarEx (2016)). There have also been increases in exploitation, with employees blackmailed both on-shore and at sea (European Cybercrime center (2014) ESC Global Security (2015)). As ships and crew physically move and connect to a wide range of local and foreign networks, there is a higher chance of insecure network connections than normal, stationary work locations.

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 (U.S. Army Criminal Investigation Command (2017a,b)). 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 (CyberKeel (2014a)). 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 cyber-risks.

Apart from the human factor there are a few more specialized systems to be address. This is an incomplete list, as ships can be highly specialized and modified, but includes some notable technologies for maritime-cyber risk. 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, as discussed in Norway (2017). 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 could be controlled through a computer terminal, e.g. in engineering. That said, engine control rooms (ECRs) are becoming increasingly dependent on growing information technology systems, as seen in Man et al (2018). Pentesting (see Section 6) is likely needed to determine specific vulnerabilities in specific cases. Another system worth mentioning is monitoring. There has been recent demands for *CCTV* like camera solutions on ships. As a common technology, it is an established system with known vulnerabilities, as seen in Costin (2016) and Heffner (2013). Cyber-attacks against monitoring may be more useful for covering up internal crimes, but may be used with sophisticated 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 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, as stated in Traub and Hudson (2007). Maliciously triggering or silencing alarms could also drastically distract and stress crew. Future work, see in Section 6, will include the engine room, as it is another area where systems are evolving and converging, likely increasing cyber-risks.

Lastly, it seems important to mention *eAtoNs*. Previously, AIS was mentioned as a ship anti-collision system. 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 (eAtoNs) have been introduced to environments where physical AtoNs are impossible or problematic to anchor. This includes coral reefs and Arctic passages where ice movements present a challenge, as described in Weintrit (2015). While not yet a widespread practice, as these virtual objects exist firmly within the cyber domain and cannot be visually, physically, checked, this could be a high-risk target for hackers seeking collision and misdirection incidences.

4 `MaCRA` Risk Assessment Examples

From the data gathered on maritime systems, attacker profiles, and possible outcomes in Sections 2 and 3, `MaCRA` can be sufficiently populated for several demonstrative risk assessments. These are designed to show complex cyber-risk information in a human-friendly format. The set of discussed vulnerabilities and their potential effects have been collated into Table 3, excluding specialized systems from Section 3.6 and those outside the scope of this study. From Table 3, $axis_s$ 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, etc. Within this study, the full set of effects considered are `damage`, `theft`, `denial of service`, `misdirect`, and `obfuscate`. As the `MaCRA` dataset grows with realistic shipping data, more types or subtypes may be considered to maintain useful assessments. $Axis_e$ and $axis_r$ 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 were specifically chosen to create interesting scenarios for `MaCRA` to assess. Sections 4.1 – 4.4 demonstrate basic projected views and filters within `MaCRA`, while Section 4.5 has a fuller discussion of `MaCRA`'s risk assessment abilities with a detailed scenario and more realistic hacker and ship data.

Table 3 System vulnerabilities and effects considered in MaCRA.

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

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

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 International Maritime Organization (2004, 2009a,b) regulations, the vast majority of ships are equipped with the systems detailed in Table 3. 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 2.4). This allows an analyst to perform realistic assessments with moderate levels of data.

4.1 Yacht Scenario: Hactivist vs Criminal

In this scenario cyber-risks of a yacht is shown. The wealth of $target_y$'s passengers makes them, and their data, of interest to criminals ($attacker_c$). In addition, local hacktivists ($attacker_h$), are concerned about boating activity in a delicate marine region. While $target_y$ is equipped with some network-defenses, the ship has several custom network-connected systems (e.g., personal entertainment), which introduces more cyber-vulnerabilities than normal. To compare the risks of $attacker_c$ and $attacker_h$ on $target_y$, these data can be modeled and extrapolated into Figure 8 to aid passenger decisions.

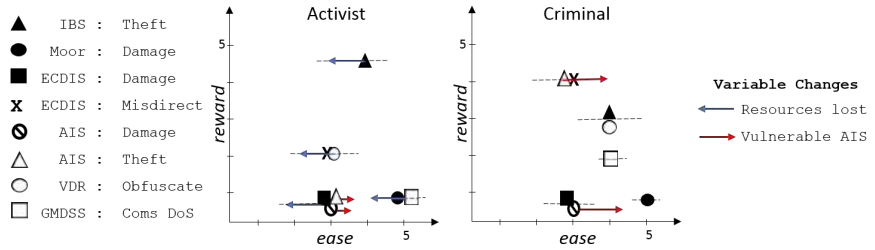


Fig. 8 Yacht risks considering activist and criminal hackers with ranged Ease-of-Exploit.

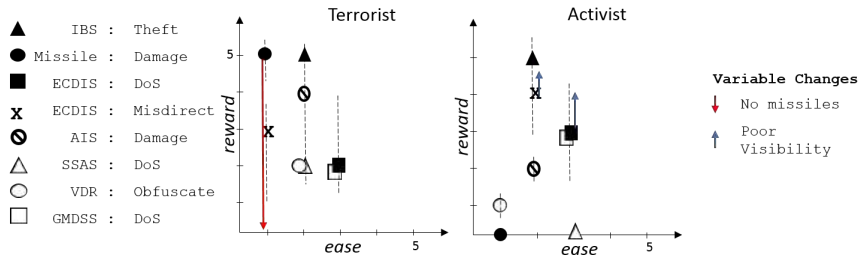


Fig. 9 Naval vessel's risk considering terrorist and activist hackers with ranged reward.

This specific view of model data shows that the top risks are information theft by $attacker_h$ via the main bridge computer, followed by misdirection and theft, physical and intellectual, by $attacker_c$ via ECDIS or AIS. Passengers can conclude $target_y$'s highest risk is information theft, as both considered hackers would find it a low-cost, high-reward attack. The view of the same data may imply different conclusions, however, if the yacht manufacture is analyzing the risks from all potential hackers including terrorists and competitors.

The Figure 8 projection of `MaCRA` model data onto a comprehensible risk plane can also help the yacht passengers quickly conclude that physical damage is low-risk and not a top priority for securing, despite the fear factor. Figure 8 also demonstrates how `MaCRA` can model ranges for attacker attributes instead of fixed values. This is useful, as the model can assess subsets of $attacker_{type}$ and different $attacker_{resource}$ levels. Human analysts, like insurers, can then compare risks associated with the best or worst case scenarios by varying variables. 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 $axis_e$. 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 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 re-assess risks, as variables change in real-time, to better inform human-based decisions. This is particularly critical when trying to assess risk when factors are quick to change. For instance, a new piece of malware may have been released or there are increased competitions between two companies. This example demonstrates that, if $attacker_h$ lost resources in a police raid, their EoE would lower. Similarly, if $target_y$ missed an important AIS security patch, the risk profile would change again. MaCRA is capable of modeling these changes, as demonstrated by the arrows in Figure 8, whether adapting to real-time changes or pre-change to help an analyst decide which security actions would most optimally and effectively decrease risk. It is that, or try to anticipate future risks.

4.2 Military Scenario: Terrorist vs Hacktivist

From an examination of military concerns, navy ships seem at most risk when considering terrorists and hactivists (i.e., $attacker_t$, $attacker_h$). For instance, 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 could be jammed. Furthermore, the underlying bridge OS is outdated which, despite additional military hardening, has some vulnerabilities. The goal of $attacker_h$ is to delay military operations in protest, whereas $attacker_t$ is interested in intelligence information and possibly compromising $target_n$'s missile weapon system.

From this scenario assessment, shown in Figure 9, the top risk based on the risk quadrants is information theft. Both modeled hackers would be interested in the data and, even if neither were, a third party would likely be. 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 risks in Figure 8. As each attacker type has sub-sets or sub-types (e.g., terrorist factions), Figure 9 supplements single tiers with ranging $attacker_{goal}$ and $attacker_{resources}$ variables 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), this assessment shall demonstrate the MaCRA framework's ability to reflect risk changes on the reward axis due change in the target. 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 into a region of low visibility, as a loss in navigation would suit $attacker_h$'s goal of delaying naval operations. This is to demonstrate an aspect of MaCRA's capabilities 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.

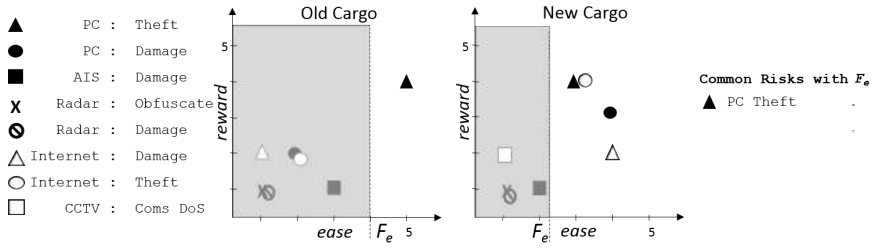


Fig. 10 Common filtered risks of a competitor hacker on both old and new cargo ships.

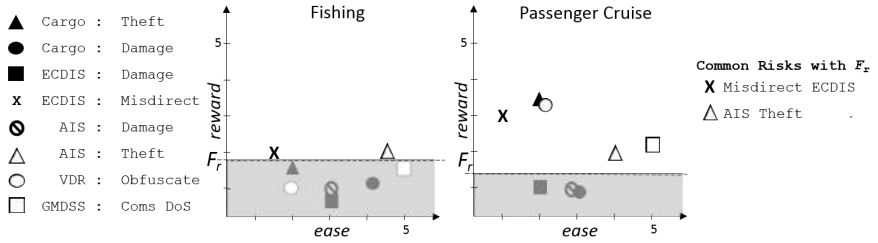


Fig. 11 Common filtered risks for fishing and cruise ships with criminal hacker.

4.3 Competitor Scenario: New vs Old Cargo Ships

In this scenario, Figure 10 projects views a company might generate to help assess the cyber-risks associated with a competitor ($attacker_c$) deploying cyber-attacks. The targeted company can also use `MaCRA` to filter out acceptable risks for optimal cyber-security investing. In this scenario one of the targeted ships is 30 years old and the other is brand new, i.e. $target_o$ and $target_n$. This illustrates how `MaCRA` assessments can highlight subtle, yet essential, target differences when considering risks, as these ships share similarities in function. While individual systems on $target_o$ may have more vulnerabilities, air gaps between non-networked systems prevent some attacks and low bandwidths decrease both `EoE` and reward for a hacker. Conversely, the newer ship has cyber-defenses, although not fully tested. This helps the hacker objectives, as its complexities and interconnectivity increase the cyber-attack surface. Within this scenario, $attacker_c$ is saboteurs on both target ships intending to steal or alter data, such as manifests and schedules.

Another tool `MaCRA` provides for real-world assessments is the ability to define acceptable and not-acceptable risks, as security solutions can be costly and most risks cannot be reduced to zero. Section 2.4 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 are based on attacker effort, sophisticated attacks are determined as acceptable risks under the assumption that they are unlikely to happen when considering the average hacker's available resources.

4.4 Criminal Scenario: Fishing vs Cruise Ship

In this scenario, MaCRA models one criminal $attacker_c$ and two targets, fishing vessel $target_f$ and cruise ship $target_c$, and assess the relevant risks from an insurer's point of view. While the international, luxury 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., $tiers_{4-5}$) and the presence of passengers would make any cyber-attack high-profile. 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, thus response the time of authorities will be short, minus a DoS attack.

A projected risk view to aid assessment can be found in Figure 11, demonstrating the use of MaCRA's reward filter 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. An insurer assessor may therefore use this filter to measure the number of non-acceptable risks when considering a cyber-risk quote.

Within this scenario, the company that owns $target_c$ has delegated 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 in Figure 11. The differently sized risk quadrants defined by these filters determine different sets of acceptable and 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 due to the non-trivial rewards for $attacker_c$. More realistically however, 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 utilized one filter each.

4.5 Other Views: Realistic Tanker Scenario

As the MaCRA framework models a plethora of information in a multi-dimensional space, there are many ways to extract the data for different people to assess scenarios based on their cyber-risk interests. Therefore the data projections in Figures 8-11 are not the only way to view the model risk-data. In this last subsection, MaCRA assessments are made with more realistic data, as shown in Table 4. While previous scenarios selected a small subset of attackers, ships, and systems to view narrow assessments and different MaCRA capabilities, all hacker profiles and systems discussed in this article are used here. As MaCRA is currently unable to model the entire global fleet, Table 4 models fictional oil tankers $target_A$ and $target_B$. Typographic differences in Figure 4 illustrate how different attributes effect the model data. Additional columns can

Table 4 A more realistic `MaCRA` 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	EoE

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

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, especially as technology evolves.

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. However, $target_B$'s ECDIS in isolation is more secure in comparison. Lastly, $target_B$'s route passes a terrorist zone and physically narrow channels that may make land-based DoS attacks more feasible. From this data `MaCRA` can, for example, use both F_e and F_r filters to identify several sets of risk. Such sets may be categorized into low-, medium-, and high-risks, or acceptable and non-acceptable. For example, consider Figure 12's four risk quadrants (i.e., $risk_q$) defined by F_e and F_r. Low risks sit in the bottom-left quadrant, medium equates to the two light gray quadrants, and the set of high-risks in the top right quadrant. Similarly, on the same figure, the three gray quadrants may be considered acceptable risks whereas the top right quadrant would remain as high, non-acceptable risks. If no filters are present, $risk_q$ may be defined by dividing the space into equal quadrants.

Similarly, the risk of each `(system : effect)` pair on $axis_s$ may be quantified by calculating its distance (i.e., $risk_d$) to the origin using risk indicator $I()$ as it was presented in Section 2. The may be done in isolation, or to rank risks within the previously defined sets. The latter is recommended, as calculating $risk_d$ alone can be misleading. For example, although the $risk_d$ of two systems may be the same, 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, despite how resource consuming a cyber-attack may seem. When considering the highest risks of $target_B$ after applying the filters F_e and F_r in Figure 12, terrorist damage ranks highest with a $risk_d$ of 32.2,

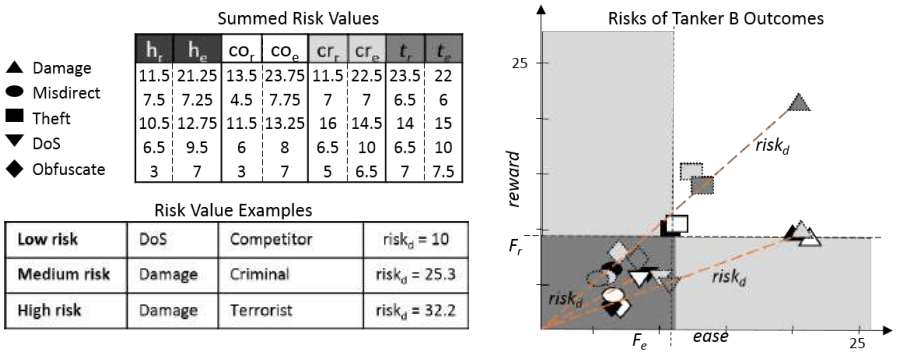
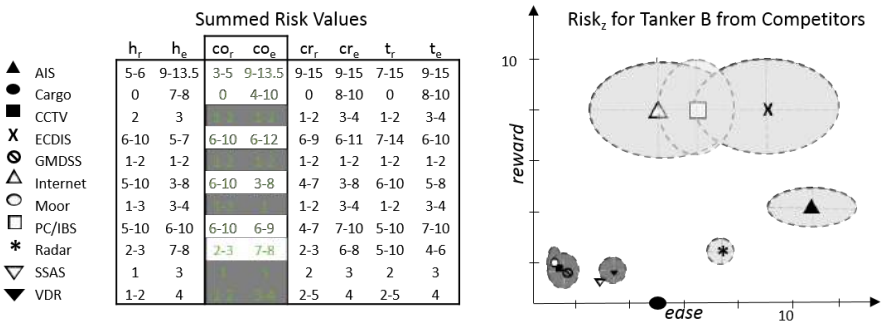


Fig. 12 Averaged summed effect risks of Tanker B with risk quadrants defined by filters.

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 4), 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 in Table 4, 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 4 so that each row represents a system's risk, despite the attack effect. This pushes technologies with multiple vulnerabilities further into the high-risk quadrant. For a human 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 2.4 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	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
Internet	5-10	3-8	6-10	3-8	4-7	3-8	6-10	5-8
Moor	1-3	3-4			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			2	3	2	3
VDR	1-2	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, dimensions can be reduced to show analysts cyber-risk pieces of the whole picture 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 and only view system components of $axis_s$, 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 person 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 6).

The last possible projected MaCRA views to discuss concerns the definition of attacker and target, i.e. equations (1) and (2). 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 this ability whall be further developed 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 re-

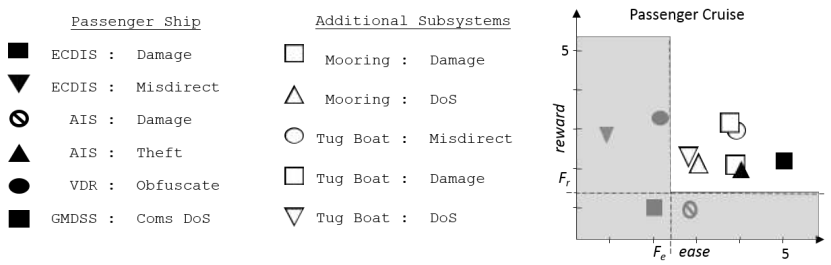


Fig. 14 Risk of ship systems and relevant subsystems of other vessels.

liably identifying acceptable and non-acceptable risks with quantified values. Assessors are also 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.

5 Related Work and Limitations

The purpose of this study is to enable a range of groups and individuals, interested in different aspects of cyber-risk, to comprehensively assess any risks maritime systems might have without excluding any technology that may seem unimportant, as ot may actually pose a large risk when considering cyber-security instead of physical or accidental. Differing from existing research, this will better enabling people to make maritime cyber-security decisions by fully understanding their risks will help focus global efforts through informed decisions. It is clear that, not only do threats and hazards need to be identified and controlled better, but they also need to be eliminated in the maritime sector, based on a mariner opinion survey in Daszuta and Ghosh (2018). To put this in to context, this section discusses how related works are dissimilar, as well as highlight what this article does not cover. This transitions into the following Section 6, "Future Work" where these limitations can be removed.

The focus of this article is not on predicting incident risks, human or machinery-based, or accident statistics, as has been done in Goerlandt and Montewka (2015); Montewka et al (2014) and Nordstrm et al (2016), 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. Balduzzi (2014); CyberKeel (2014a); Latin America & Caribbean (2014); Mordechai et al (2014); Schmidt et al (2016); Trend news agency (2012); Wagstaff (2014) and Suh (2014) 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.

Other recent studies focused on individual systems, not "systems of system 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 ships by the Marine accident investigation branch (2012, 2014); Wagstaff (2014) and Vandenborn and Bell (2015). 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 (CyberKeel (2014b); Dyryavyy (2014); Santamarta (2015)). Several of these studies overlap with other areas of concern, such as navigation in airplanes or cars (Bordonali et al (2017); Control (2015); Snyder et al (2015); Yeomans (2014)), and the SCADA systems of smart grids and railways (Collins (2017); Leyden (2016); Safa et al (2016)).

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 past maritime-based studies like Lane et al (2010) consider risk, they only analyze it for one particular factor, as opposed to evaluating an entire ship or fleet, as `MaCRA` aims to do. For example, Committee and Harwood (2015); Danish Defence Intelligence Sevice's Center for Cyber Security (2014) focused on attacker assessments and Bateman (2010); Nankivell et al (2017) assessed specific geographical regions where cyber-crimes are prevalent.

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 (see den Braber et al (2007); Cherdantseva et al (2016); Lund et al (2010); NIST (2012); Sommestad et al (2013)). Based on this, 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`. For example, `MaCRA` can incorporate more detailed insider-threat models, such as Cappelli et al (2012); CERT Insider Threat Center (2014).

Like some previous tools, e.g. Lund et al (2010), `MaCRA` primarily present data visually. Studies have found this a more intuitive and effective way to evaluate risks, Labunets et al (2014); Stålhane and Sindre (2014), which is why `MaCRA` provides risk zones and quadrants (i.e., $risk_z$ and $risk_q$) for a better human experience. However, quantified values are also available as risk measurements (i.e., $risk_d$). Thus `MaCRA` is able to produce results 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.

This is the first proposal for a framework designed specifically to assess changin 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 2, 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 cyber-risks and project useful views for informed human security decisions.

6 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, `MaCRA` will be suitably populated for real-world usage, as it was in Tam and Jones (2018a) for assessing cyber-risks specific autonomous ships.

There are many vulnerable systems in the maritime sector and while they have primarily resulted in accidents, these vulnerabilities may be intentionally exploited with cyber-attacks. This paper has enumerated a large set of such vulnerabilities and outcomes in Sections 3 and 4. 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. Fully understanding maritime-cyber risks would be able to inform policy-making changes and additions holistically. An early demonstration of this can be found in Tam and Jones (2018b), however as risk becomes better understood future policy work can be much more detailed and effective.

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, such as Cappelli et al (2012); CERT Insider Threat Center (2014); Rios Insua et al (2016), 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 smartphones 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 and ports, 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, as stated in International Chamber of Shipping (2016), 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.

7 Conclusions

This paper proposes a maritime cyber-risk assessment (MaCRA) framework to be used by companies, organizations, and individuals to assess cyber-risks given any possible maritime-cyber scenario, i.e. any combination of ship, system, environment, and attacker, in the unique maritime context. More importantly, by fully populating the proposed model with real-world data and creating an array of, human-friendly, customizable views, one can discover risks not previously considered. The framework can also adapt as maritime technology evolves and as attackers find new vulnerabilities and incentives. This is not currently feasible when only assessing one attacker or system at a time, which is the approach of most previous research. Moreover, similar cyber-risk assessment frameworks are not well suited to the unique maritime environment. This led to the development of MaCRA, to provide accurate and quantifiable cyber-risk assessments, enabling the maritime community to identify the most significant maritime-cyber risks with enough detail to 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 increase crew safety, general cyber-security, enable significant cost savings on cyber protection investment, and inform accurate assessments for maritime crew, businesses, cyber-risk insurers, policy makers, and 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.

8 Acknowledgments

The authors would like to express their great appreciation to Tom Crichton, Captain Robert Hone, and Steven Furnell from the University of Plymouth for their assistance and guidance throughout this paper.

References

Allianz Global Corporate and Specialty SE (2016) Safety and shipping review 2016. Allianz Global Corporate and Specialty

Archives UN, Administration R (2016) CFR Title 47 (parts 80-end) code of federal regulation title 47 telecommunications revised as of october 1, 2016. Code of Federal Regulations (CFR)

Balduzzi M (2014) AIS exposed understanding vulnerabilities & attacks 2.0. BlackHat

Bateman S (2010) Regional maritime security: threats and risk assessments. University of Wollongong

BBC News (2009) Nuclear subs collide in atlantic. BBC

BigOceanData (2016) AIS and anti-piracy maritime security. BigOceanData

BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO (2016) The guidelines on cyber security onboard ships v2.0. International Chamber of Shipping

Bordonali C, Ferraresi S, Richter W (2017) Shifting gears in cyber security for connected cars. McKinsey&Company Advanced Industries

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

den Braber F, Hogganvik I, Lund MS, Stølen K, Vraalsen F (2007) Model-based security analysis in seven steps — a guided tour to the coras method. BT Technology Journal

Cappelli D, Moore A, Trzeciak R (2012) The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Addison-Wesley

Cassidy W (2017) China-based cyberattack hits logistics operators, shippers. Outsource, volume 5 issue 6

Cavotec (2014) Moormaster frequently asked questions. Cavotec

CERT Insider Threat Center (2014) Unintentional insider threats: Social engineering. Tech. Rep. CMU/SEI-2013-TN-024, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA

Cherdantseva Y, Burnap P, Blyth A, Eden P, Jones K, Soulsby H, Stoddart K (2016) A review of cyber security risk assessment methods for scada systems. Computers & Security 56

Coffed J (2014) The threat of gps jamming. Exelis

Collier E (2017) eLoran: More accurate & less vulnerable but not a done deal yet. Marine electronics

Collins R (2017) The state of cybersecurity in the rail industry. White paper

Committee JH, Harwood S (2015) Cyber risk. Joint Hull Committee (JHC)

Control CAT (2015) Cyber security project. `www.csfi.us`

Costa NA, Jakobsen JJ, Weber R, Lundh M, MacKinnon SN (2018) Assessing a maritime service website prototype in a ship bridge simulator: navigators' experiences and perceptions of novel e-navigation solutions. WMU Journal of Maritime Affairs DOI 10.1007/s13437-018-0155-2

Costin A (2016) Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. In: Proceedings of the 6th Interna-

tional Workshop on Trustworthy Embedded Devices
CyberKeel (2014a) Maritime cyber-risks. NCC Group Publication
CyberKeel (2014b) Security risks and weaknesses in ecdis systems. NCC Group Publication
Danish Defence Intelligence Sevice's Center for Cyber Security (2014) Threat assessment: The cyber threat against the maritime sector. Marine Cyberwatch
Daszuta W, Ghosh S (2018) Seafarers' perceptions of competency in risk assessment and management: an empirical study. WMU Journal of Maritime Affairs DOI 10.1007/s13437-018-0156-1
Degani A (2004) Taming HAL: Designing Interfaces Beyond 2001. Springer
Dyryavyy Y (2014) Preparing for cyber battleships: Electronic chart display and information system security. NCC Group Publication
ECDIS Info (2014) ECDIS Regulations. http://www.ecdis-info.com/ecdis_regulations.html
European Cybercrime center (2014) The internet organised crime threat assessment (iOCTA). European Police Office
Fitch C (2004) Crime and punishment: The psychology of hacking in the new millennium. SANS Institute
Francillon A, Danev B, Capkun S (2011) Relay attacks on passive keyless entry and start systems in modern cars. Network and Distributed System Security Symposium
Franckx E (2001) 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
Goerlandt F, Montewka J (2015) Maritime transportation risk analysis: Review and analysis in light of some foundational issues. Reliability Engineering & System Safety
GPS World staff (2016) US coast guard issues gps jamming alert. GPS World
Grant A, Williams P, Basker S (2014) GPS jamming and the impact on maritime navigation. The General Lighthouse Authorities
Heffner C (2013) Exploiting surveillance cameras like a hollywood hacker. Tactical Network Solutions
Igure VM, Laughter SA, Williams RD (2006) Security issues in scada networks. Computers & Security
IMO Navigation (2017) http://www.imo.org/en/OurWork/Safety/Navigation/, accessed: 2017-05-17
International Chamber of Shipping (2016) Review of maritime transport. United Nations Conference on Trade and Development (UNCTAD)
International Maritime Organization (1974) International convention for the safety of life at sea. IMO
International Maritime Organization (2004) Solas chapter V annex 17: Automatic identification systems (AIS). IMO
International Maritime Organization (2009a) Solas ch V regulation 19: Carriage requirements for shipborne navigational systems and equipment. IMO

International Maritime Organization (2009b) Solas chapter V regulation 19-1: Long range identification and tracking of ships. IMO

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

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

Labunets K, Paci F, Massacci F, Ruprai R (2014) An experiment on comparing textual vs. visual industrial methods for security risk assessment. In: 2014 IEEE 4th International Workshop on Empirical Requirements Engineering (EmpiRE)

Lane RO, Nevell DA, Hayward SD, Beaney TW (2010) Maritime anomaly detection and threat assessment. 13th International Conference on Information Fusion

Latin America & Caribbean (2014) Seized n korean ship: Cuban weapons on board. BBC

Leyden J (2016) Water treatment plant hacked, chemical mix changed for tap supplies. The Register

Lund MS, Solhaug B, Stlen K (2010) Model-Driven Risk Analysis: The CORAS Approach. Springer Publishing Company, Incorporated

Maersk (2017) A. P. Moller Maersk improves underlying profit and grows revenue in first half of the year. Maersk URL `https://edit.maersk.com/en/the-maersk-group/press-room/press-release-archive/2017/8/a-p-moller-maersk-interim-report-q2-2017`

Man Y, Lundh M, MacKinnon SN (2018) Managing unruly technologies in the engine control room: from problem patching to an architectural thinking and standardization. WMU Journal of Maritime Affairs DOI 10.1007/s13437-018-0159-y

MarEx (2016) Nigerian navy: Crewmembers involved in pirate attacks. The Maritime Executive

Marine accident investigation branch (2012) Grounding of CSL THAMES in the Sound of Mull 9 august 2011. Marine accident investigation branch (MAIB)

Marine accident investigation branch (2014) Report on the investigation of the grounding of Ovit in the Dover Strait on 18 september 2013. Marine accident investigation branch (MAIB)

Marine Accident Investigation Branch (MAIB) (1997) Safety digest 02/1997. `gov.uk`

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

MOOREX M (2014) Mooring and auto-mooring solutions. ShipServ

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

Nankivell KL, Reeves J, Pardo RP (2017) 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)

National PNT Advisory Board (2010) Jamming the global positioning system: A national security threat recent events and potential cures. General Lighthouse Authorities

NIST (2012) Guide for conducting risk assessments - information security. NIST Special publication 800-30

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

Norway MP (2017) Inert gas system (IGG). Maritime Protection AS

Offshore Blue (2013) Tales of the unexpected. The Navigator: Inspiring professionalism in marine navigators

Offshore Blue (2016) A re-cap of the navtex system. Navigator's Newsletter

Peltier TR (2005) Information security risk analysis. Auerbach Publishing

Rios Insua D, Banks D, Rios J (2016) Modeling opponents in adversarial risk analysis. Risk Analysis

Rolls Royce (2017) Autonomous ships: The next step. Marine Ship Intelligence

Rothblum A (2000) Human error and marine safety. International Workshop on Human Factors in Offshore Operations (HFW2002)

Safa HH, Souran DM, Ghasempour M, Khazaee A (2016) Cyber security of smart grid and scada systems, threats and risks. In: CIRED Workshop 2016

Santamarta R (2014a) Satcom terminals: Hacking by air, sea, and land

Santamarta R (2014b) A wake-up call for satcom security. IOActive

Santamarta R (2015) Maritime security: Hacking into a voyage data recorder (VDR). IOActive

Schmidt D, Radke K, Camtepe S, Foo E, Ren M (2016) A survey and analysis of the gnss spoofing threat and countermeasures. ACM Comput Surv

SeaCert (2016) Global maritime distress and safety system (GMDSS) radio operator. Maritime NZ

ESC Global Security (2015) Maritime cyber security white paper: Safeguarding data through increased awareness. ESCGS Cyber Security White Papers

Simon H, Ray H (2005) A taxonomy of network and computer attacks. Computers and Security

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

Sommestad T, Ekstedt M, Holm H (2013) The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. IEEE Systems Journal

Stålhane T, Sindre G (2014) An experimental comparison of system diagrams and textual use cases for the identification of safety hazards. Int J Inf Syst Model Des

Suh J (2014) The failure of the south korean national security state
Tam K, Jones K (2018a) Cyber-risk assessment for autonomous ships. IEEE TCS Cyber Security
Tam K, Jones KD (2018b) Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. DOI 10.1080/23738871.2018.1513053
Traub P, Hudson R (2007) Alarm management strategies on ships bridges and railway control rooms, a comparison of approaches and solutions. Paper read at RINA Event, at London
Trend news agency (2012) Iran oil tankers said by zanzibar to signal wrong flag. Bloomberg
United States General Accounting Office (1999) Information security risk assessment practices of leading organizations. GAO/AIMD-98-68
US Army Criminal Investigation Command (2017a) Cyber sextortion. CPF 0002-17-CID361-9H
US Army Criminal Investigation Command (2017b) Cybersecurity: Sextortion exploitation of u.s. service members. U.S. Army Criminal Investigation Command
US Department of Homeland Security (2015) Gps and critical infrastructure. Civil GPS Service Interface Committee
USMRC Maritime Cyber Assurance Research (2016) The reality of shipboard cyber vulnerabilities. USMRC Maritime Cyber Assurance Team (MCAT)
Vandenborn Y, Bell R (2015) Standard safety special edition - ECDIS assisted grounding. Marine accident investigation branch (MAIB)
Wagstaff J (2014) All at sea: Global shipping fleet exposed to hacking threat. Reuters
Weintrit A (2015) Activities in Navigation: Marine Navigation and Safety of Sea Transportation. Taylor & Francis Group
Wingrove M (2016) Lack of training causes ship accidents and detentions. Marine Electronics & Communications
Yeomans G (2014) Autonomous vehicles handing over control: Opportunities and risks for insurance. Lloyd's
Zhang J, Ioannou P (2006) Automated container transport system between inland port and terminals. ACM Transactions on Modeling and Computer Simulation