Preventing Catastrophic Cyber-physical Attacks on the Global Maritime Transportation System: a case study of hybrid maritime security in the Straits of Malacca and Singapore

Adam James Fenton *

Posted Date: 22 January 2024

doi: 10.20944/preprints202401.1609.v1

Keywords: maritime security; cybersecurity; maritime governance; Southeast Asia; cybercrime; cybersecurity governance

Article

Preventing Catastrophic Cyber-Physical Attacks on the Global Maritime Transportation System: A Case Study of Hybrid Maritime Security in the Straits of Malacca and Singapore

Adam James Fenton

ad8938@coventry.ac.uk

Abstract: This paper examines hybrid threats to maritime transportation systems, and their governance responses; focusing on the congested Straits of Malacca and Singapore (SOMS) as an illustrative case study. The methodology combines secondary sources with primary data from 42 expert interviews, a 30-respondent survey, and two maritime security roundtables. Key findings were that ships' critical systems are increasingly interconnected, yet aging IT infrastructure and minimal cybersecurity awareness among crews heighten risks. Meanwhile, regional terrorist groups have previously targeted shipping and shown considerable skill in exploiting online tools, aligning with broader calls for jihadist violence. Further, opportunistic piracy persists in the SOMS with the potential to disrupt shipping. Experts confirmed maritime cybersecurity lags other critical infrastructure sectors and needs updated governance. Initial International Maritime Organization (IMO) guidelines lack specificity but revisions and updated IMO guidance are in process, while Port state implementation of maritime cybersecurity standards varies. Crucially, information sharing remains inadequate, even as recorded attacks increase. Findings underscore that although major hybrid incidents have not occurred, simulations and threat actors' capabilities demonstrate potential for catastrophic collisions or cascading disruption in congested waterways. Mitigating factors like redundancy and crew training are deficient currently. Some alignment between SOMS states on maritime security cooperation exists, but not cyber threats specifically. Key recommendations include an anonymous cyber-attack reporting system, reinforced training and shipboard systems, and consolidated regional frameworks. Until these priorities are addressed, the analysis concludes that hybrid vulnerabilities in this vital global chokepoint remain a serious concern.

Keywords: keyword 1; maritime security 2; cybersecurity 3 maritime governance 4 Southeast Asia 5 cybercrime

1. Introduction

Incidents such as an escalation of Houthi attacks on shipping through the Red Sea [1], blockage of the Suez Canal by M.V. Ever Given in 2021 [2] and the paralysing malware attack on shipping giant Maersk in 2018 [3], underscore both the critical importance of the maritime transportation system (MTS) to global supply chains and its acute vulnerability to disruptive kinetic, cyber, or cyber-physical attack. This article will discuss hybrid threats to the MTS in response to three broad research questions: first, what are the greatest hybrid threats to maritime security, taking account of the unique nature of Information Technology (IT) and Operational Technology (OT) systems in ships? Second, who are the most likely non-state actors to exploit such weaknesses and what are the likely attack vectors? Third, what governance regimes exist at the intersection of maritime security and cyber security to protect or mitigate against hybrid attacks on shipping? As a lens through which to view and discuss hybrid maritime security and its governance the article focusses on shipping through one of the world's most congested shipping chokepoints, the Straits of Malacca and Singapore (the "SOMS"). Due to the transnational nature of global shipping and its governance mechanisms, many

 doi:10.20944/preprints202401.1609.v1

of the lessons taken from this discussion will be relevant and applicable to hybrid maritime security in other strategic global chokepoints, such as, the Bab Al Mandeb strait, Suez Canal, Panama Canal and others [4]. Survey results indicate strong support for several key findings: (1) Information and Communication Technology (ICT), networked devices and emerging technology on board ships creates new challenges for maritime security (2) current levels of cybersecurity in ships are insufficient (3) criminal cyber attacks on the maritime sector have occurred in the past and will continue to be exploited by criminal groups (4) cybersecurity in the maritime sector lags behind other sectors and (5) current regulations are insufficient to address challenges posed by new technology. The article concludes that a number of factors contribute to vulnerabilities of ships to cyber-attack – a convergence of IT and OT systems, greater connectivity through Low Earth Orbit (LEO) satellites, outdated legacy software and hardware, and a paucity of information sharing about cyber-attacks in the maritime sector. Likely attack vectors in the maritime sector include all of the same threats to land-based businesses – ransomware, phishing, Business Email Compromise (BEC) – and several more that are unique to the sector; malware capable of disabling a ship's navigational interfaces or critical OT systems such as steering and engines, and/or AIS/GPS spoofing or jamming causing confusion and potential for collisions at sea. Further, regional threat actors in Southeast Asia have in the past sought to disrupt shipping and a number of key attacks on regional shipping are examined. Meanwhile, regional threat actors show a greater proficiency in the use of digital technology to achieve their goals. However, whereas some incidents of cyber-physical interference on ships' critical systems have been recorded, to date there has not been a catastrophic cyber-physical attack on shipping, but such attacks are theoretically proven to be possible and have been simulated in laboratory tests. Finally, some international governance measures are underway to mitigate hybrid threats to shipping, but they are in the early stages of development and need to be further consolidated through key bodies like the IMO and leading national governments such as the UK, US, and EU – some recommendations are made in this regard.

1.1. Methodology

Methodology for the article combines secondary sources including academic articles, international law texts such as the International Safety Management code (ISM), the Safety of Life at Sea convention (SOLAS), other international maritime treaties, case law, media reports, grey literature, and data from the Maritime Cyber Attack Database (MCAD) compiled by NHL Stenden University of Applied Sciences, Netherlands.

Primary data were collected through 42 interviews with, government and regulators, representatives from national government agencies and NGOs in the littoral states of Indonesia, Singapore and Malaysia, including; the National Maritime Institute (NAMARIN Indonesia), the Indonesian Coast Guard agency (Badan Keamanan Laut, BAKAMLA), Indonesian National Police (POLRI), the Maritime Institute of Malaysia (MIMA), the S. Rajaratnam School of International Studies (RSIS) Singapore, as well as other representatives from industry, academia, independent researchers and authors, in UK, Europe, and Southeast Asia. Further, an online survey was conducted utilising the Joint Information Systems Committee (JISC) platform. Responses were requested only from respondents who had expert knowledge of maritime security and for that reason participants were invited to complete the survey via LinkedIn professional groups and JISC professional Maritime Security mailing list (maritimesecurity@jiscmail.ac.uk). As a result, the survey was completed by 30 practitioners, experts and academics working in the field of maritime security. The research project also organised two roundtable discussions with experts in maritime and cybersecurity and related fields, one focussed on international maritime governance, and one focused on hybrid maritime security and governance in the SOMS littorals of Indonesia, Singapore and Malaysia. Each roundtable was attended by five key informant discussants with specific expert knowledge of the areas discussed. Some excerpts from these discussions are used to inform this article.

1.2. Terminology

In this paper these terms are used as follows: "kinetic" refers to actions, forces, or movements in the physical world. It commonly denotes phenomena involving actual motion or energy transfer. "Cyber" pertains to the virtual or digital domain, encompassing activities, systems, or elements related to computers, information technology, networks, and digital communication. "Cyber-physical" describes the integration or intersection between the cyber (digital) and physical (real-world) domains. It signifies systems, technologies, or environments where digital components interact with and impact physical entities. In the maritime sector, IT systems which interact with OT systems, such as rudders, engines, ballast, causing and monitoring physical motion and energy transfer, are good examples of systems that are cyber-physical. Similarly, the term "hybrid" is used to refer to a combination or fusion of digital (cyber) and physical elements within a single system or environment. It implies a convergence of technologies where digital components interact with physical entities. A hybrid attack on shipping is one that involves elements of cyber and physical vectors: a criminal group that hacks the data base of a shipping company to search for high value cargo, then boards a specific vessel at sea and uses bar code readers to physically search for the targeted cargo (based on a real incident [5]) is an example of a hybrid mode of attack.

2. Cyber Threats to Shipping

The complex "system of systems" [6] that comprises the global Maritime Transportation System (MTS) is critical to the smooth running of global trade and commerce. In the words of the UN Conference on Trade and Development (UNCTAD), it is "the backbone of international trade and the global economy" [7]. As is often noted in discussions around maritime security and "sea blindness" [8] "around 90% of traded goods are carried over the waves" [9]. If the MTS were to suffer a catastrophic breakdown it could potentially result in severe disruption to global supply chains and concomitant economic, political and social disorder. Key stakeholders are now beginning to understand the MTS's growing dependence on complex digital and automated systems [10–12], and the vulnerabilities of those systems to malicious cyber-physical interference [13] capable of causing a catastrophic collision or simultaneous cascading disruption to fleets of ships, or a major port. It is the kind of risk that is beginning to garner serious attention from leading national governments, the maritime sector broadly, international bodies like the IMO, and the insurance sector that is being called upon to underwrite the risk.

The pursuit of enhanced efficiency, decarbonization, cost reduction, and improved safety necessitates technological solutions. In the words of UNCTAD: "beyond cleaner fuels, the industry needs to move faster towards digital solutions like AI and blockchain to improve efficiency as well as sustainability" [7]. Enormous investment is being poured into developing autonomous ships [14–19], and other ways AI can be applied to the MTS [20,21]; such as improved ship design, streamlining work processes, automated monitoring of critical systems like engines, ballast and navigation, and optimised voyage planning to name a few. While automation can improve efficiency, situational awareness, and safety, the increasing dependence on networks comprising sensors, communication, and Internet of Things (IoT) devices, is driving a *convergence* of IT and OT. In the words of leading UK researchers "this convergence can provide useful monitoring and fine-grained control, sometimes even remotely, but also increases the possibility a cyber-attack could have physical consequences" [22].

Kinetic impacts on a ship's OT have been demonstrated in the laboratory proving a capability to alter the rudder angle and engine function. Using a known Common Vulnerability and Exposure (CVE) and a firmware update attack on a Programmable Logic Controller (PLC) the malicious firmware is able to use geo-fencing to define the entry coordinates to a port and begin to manipulate NMEA[1] data. A number of simulated studies have attempted to estimate the potential economic

[1] The National Marine Electronics Association (NMEA) NMEA 0183 and NMEA 2000 are standards for electronic communication between devices in ships. NMEA allows equipment to exchange information over a single communication network allowing the integration of multiple devices including navigation, sensors, engine monitoring and others.

 doi:10.20944/preprints202401.1609.v1

impacts of the shutdown of a major port or strait, such as Seville or the Straits of Malacca and Singapore (the SOMS) [23,24]. A real-world demonstration of the enormous knock-on effects and economic costs from a blockage of a major chokepoint came with the grounding of the giant container ship *M/V Ever Given* in 2021 [2]. While some have speculated that the *Ever Given* grounding could have been due to a cyber-attack [25] the official report concluded that the root cause of the incident was "loss of maneuverability of the ship" due to "wind speed, wind direction, squat, bank suction" and communication difficulties between the two pilots and the master and bridge crew [26]. Regardless of the cause, losses from the grounding were estimated at $400m (£290m) per hour or $9.6bn (£7bn) in trade and goods per day [2]. In comparison to the Suez canal which has around 50 ships transiting each day, the SOMS has around 90,000 ships per year or up to 300 ships per day [27] which would make a blockage potentially six times worse by volume.

Multiple sources confirm that disruptive attacks on shipping using cyber and cyber-physical attack vectors are increasing and evolving. The Maritime Cyber Attack Database[2] (MCAD) [28] compiled by researchers at NHL Stenden University, Netherlands, provides an interactive global representation of open-source discrete cyber-attacks on the maritime transportation sector. At the time of writing it catalogues around 165 incidents of cyber-attack on the MTS with further attacks being added through continuous updating.

Given the sometimes secretive nature of responses to cyberattack, the creators of the MCAD admit that these open-source recorded incidents are just the "tip of the iceberg" [28,29] This foreshadows one of the main challenges in maritime cybersecurity, a lack of information sharing, discussed further below.

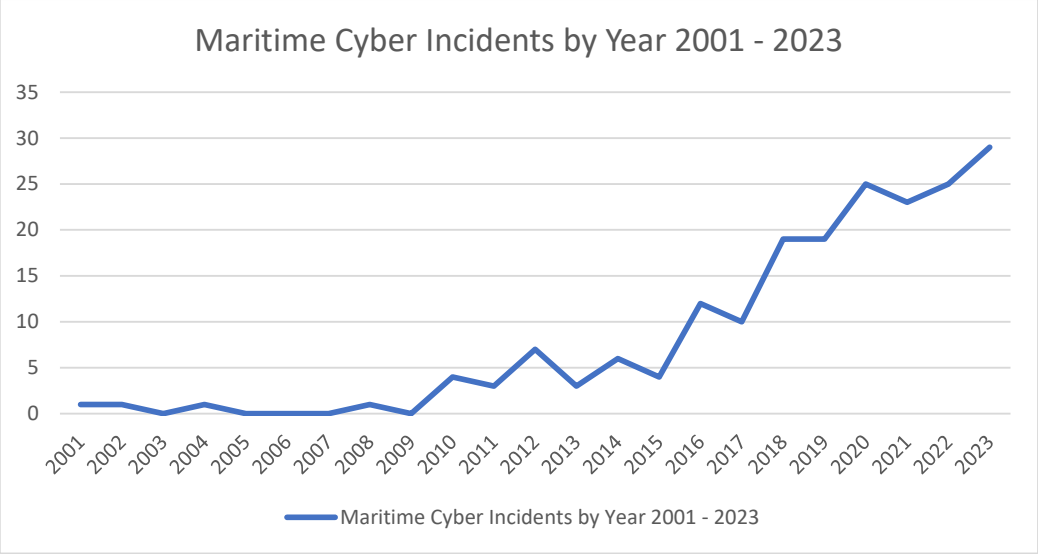

Figure 1. Maritime Cyber Incidents by Year 2001 - 2023. Recreated by author based on data from Maritime Cyber Attack Database (MCAD) NHL Stenden University, Netherlands www.maritimecybersecurity.nl.

On the evolving nature of attacks, maritime cybersecurity expert Gary Kessler commented:

One of the things that has really dramatically changed over the years is the attacker's strategy. In the old days, attacks tended to be opportunistic, if an attacker could get into your network, they would immediately roll over a server, they would deface a website, put up some porn, that sort of stuff. But attackers don't do that anymore, and they haven't done that for at least a decade. If attackers can get into your network now, they basically sit and they exfiltrate data, perhaps they do destroy a server or take you off the air, but they do it at a time of their choosing, and we've had all sorts of examples of this from the last couple of years. [30]

[2] https://maritimecybersecurity.nl/

A number of notable attacks on the MTS in recent years include: a ransomware attack on "well-established IT consulting firm" Danaos, which "hit multiple Greek shipping companies" in November 2021 [31]; cruise line operator Carnival Corp was fined $5 million for "significant" cybersecurity violations, following four security breaches from 2019 to 2021 [32]; a "serious cyberattack" which "disrupted operations at several of Australia's largest ports, causing delays and congestion" in November 2023 [33]; multiple cyber-attacks on northern European ports in Germany, Netherlands and Belgium "targeting the region's oil operations" [34]; cyberattacks on merchant ships off the coast of Somalia by pirate groups able to remotely disable ships transiting past Djibouti [28], and the oft-cited Notpetya attack on Maersk in 2018 [35]. Other notable categories of attack on the MTS are spoofing of Automatic Identification System (AIS) signals [3,36], and GPS jamming including mass jamming of GPS signals of South Korean vessels allegedly by North Korea [37], hybrid pirate attack combining hacking of a shipping company's database then boarding a vessel transiting the SOMS and using bar code readers to target specific containers on the ship [5], and spoofing of AIS signals of two NATO warships to make it appear as though they were approaching a Russian naval base [38,39]. As one of the compilers of the MCAD explained in interview "there were some challenges around how you discretely define an incident … one of the common things that happens is ships 'going dark' where they turn their AIS off. If you tracked each one of those as individual incidents, there would be thousands of those alone" [29]. The approach of the MCAD is therefore, where a similar attack is perpetrated simultaneously from the same source on multiple targets it is recorded as a single incident.

Finally, as with other land-based industries, cyber-criminal activities such as phishing, Business Email Compromise (BEC), and ransomware are equally as damaging to the maritime sector. Some research indicates that specific targeting of maritime businesses is increasing, and that the frequency and amounts of ransomware payments are increasing with one 2023 report recording that "the average cost of a ransom payment is US $3.2m" [40]. Several sources noted a lack of information sharing. On the need for sharing of cyber threat intelligence, Kessler noted: "Cyber-attacks are all exploiting vulnerabilities. What we need in the industry is better information sharing of the vulnerabilities…we have some agencies that are doing that in a small way now. But we need to really need to improve that. [30]

While mandatory reporting of cyber incidents may not be feasible or desirable, a mechanism for voluntary, anonymous reporting of cyber incidents would be a positive development for cybersecurity, and could possibly be introduced on the back of the MCAD and the Structured Threat Information Expression (STIX[3]) format for reporting cyber threat intelligence.

2.1. Survey results

Based on survey data from practitioners and academics specialising in maritime security, 93% of respondents agreed or strongly agreed with the statement "ICT (Information and Communications Technology) in ships, that is, automated, computer-based systems such as Electronic Chart Displays (ECDIS), Automatic Identification Systems (AIS), satellite communications, on-board networks of Information Technology (IT) and Operational Technology (OT) and others, create new threats, vulnerabilities and challenges for maritime security".

Further, while this article will not give detailed consideration to emerging technology such as autonomous ships, it is worth noting that 90% of respondents agreed or strongly agreed with the statement "Emerging technology – such as autonomous 'uncrewed' or 'unmanned' ships, automated, computer-based processes, machine learning, SCADA, sensors, algorithms etc., operating on board ships – create new threats, vulnerabilities and challenges for maritime security".

Survey results are presented in Figures 2–8 and discussed, with some direct quotations from respondents, below.

[3] https://stixproject.github.io/about/

 doi:10.20944/preprints202401.1609.v1

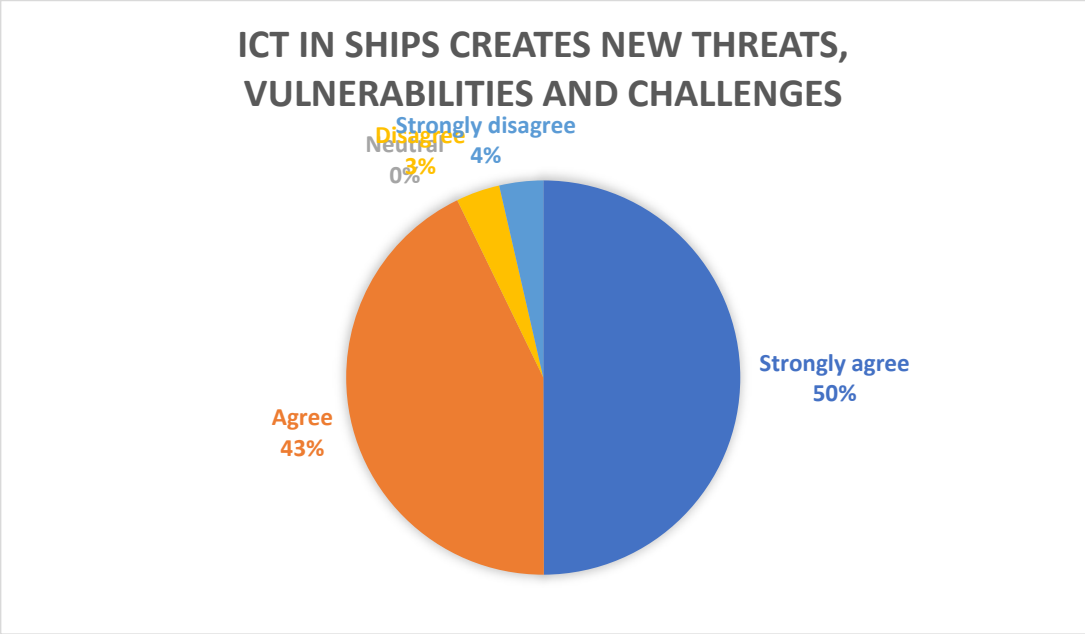

Figure 2. Survey responses to the statement "ICT (Information and Communications Technology) in ships, that is, automated, computer-based systems such as Electronic Chart Displays (ECDIS), Automatic Identification Systems (AIS), satellite communications, on-board networks of Information Technology (IT) and Operational Technology (OT) and others, create new threats, vulnerabilities and challenges for maritime security".

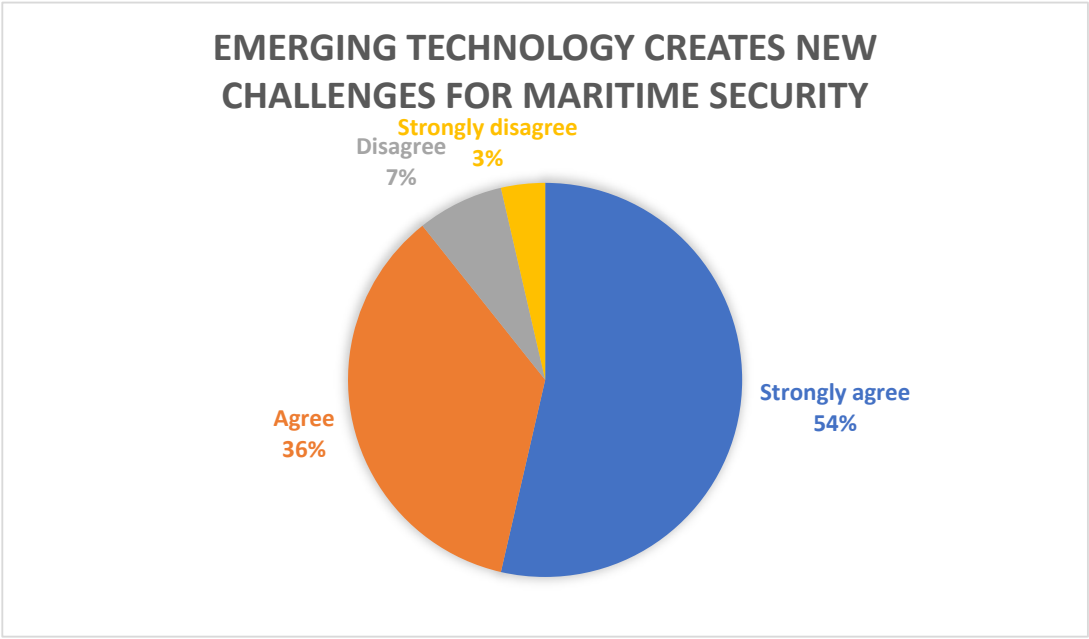

Figure 3. Survey responses to the statement "Emerging technology – such as autonomous 'uncrewed' or 'unmanned' ships, automated, computer-based processes, machine learning, SCADA, sensors, algorithms etc., operating on board ships – create new threats, vulnerabilities and challenges for maritime security".

 doi:10.20944/preprints202401.1609.v1

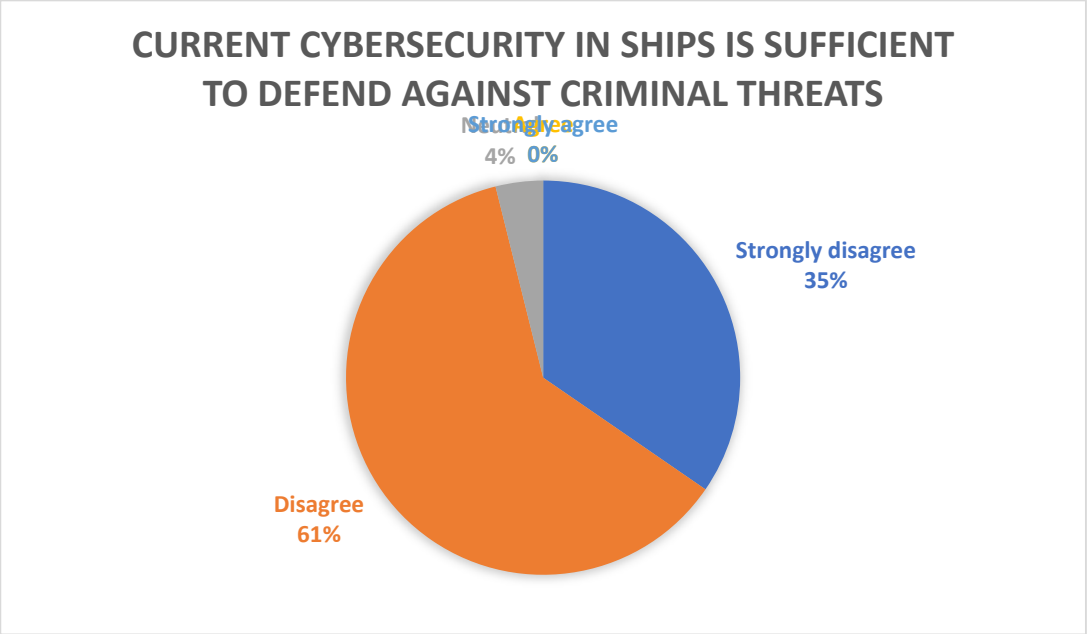

Figure 4. Survey responses to the statement "Current levels of cybersecurity in ships are sufficient to counter or defend against threats from criminal groups".

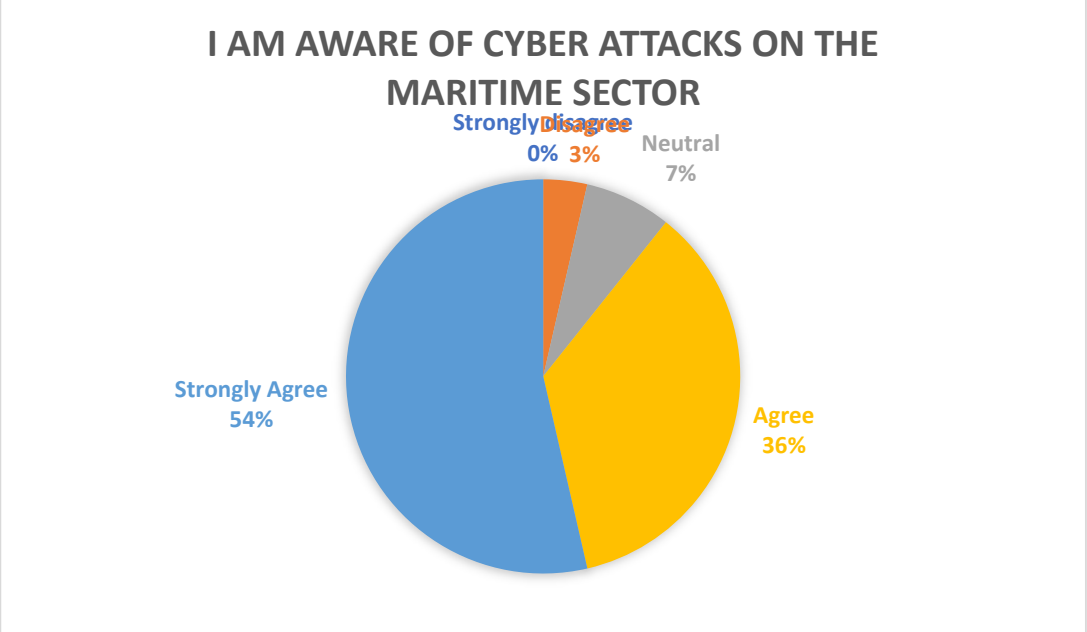

Figure 5. Survey responses to the statement "I am aware of cyber-attacks that have occurred against the maritime sector, including ships, ports and shipping companies".

 doi:10.20944/preprints202401.1609.v1

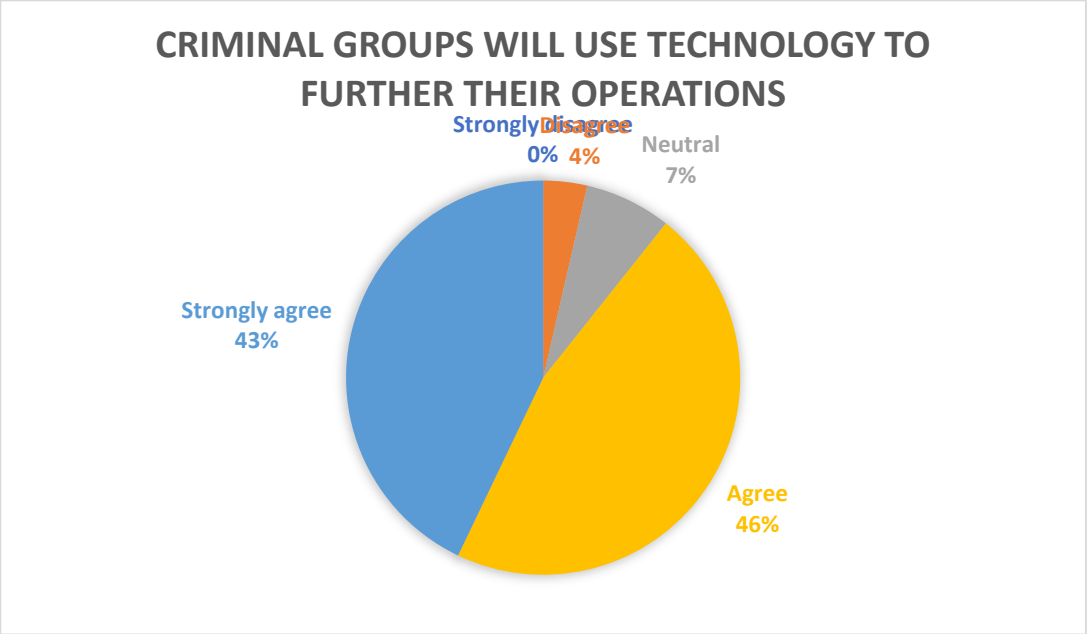

Figure 6. Survey responses to the statement "Pirate, terrorist or transnational organised criminal groups will utilise these kinds of new technology (autonomous craft, AI, cyber-attacks) to further their criminal operations".

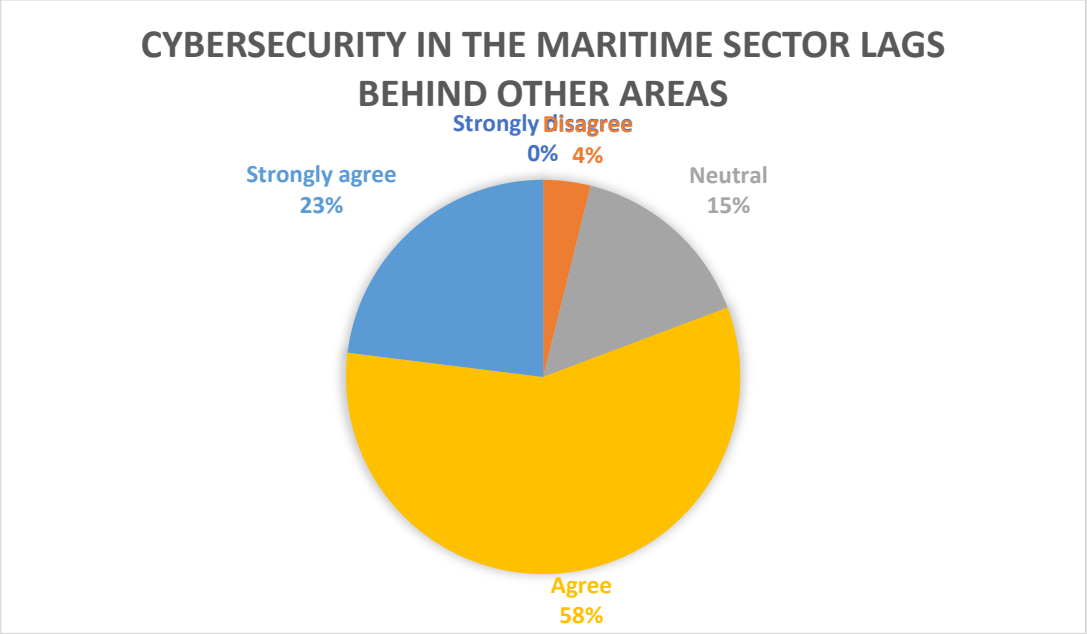

Figure 7. Survey responses to the statement "Cybersecurity in the maritime sector lags behind cybersecurity in other areas of critical infrastructure".

 doi:10.20944/preprints202401.1609.v1

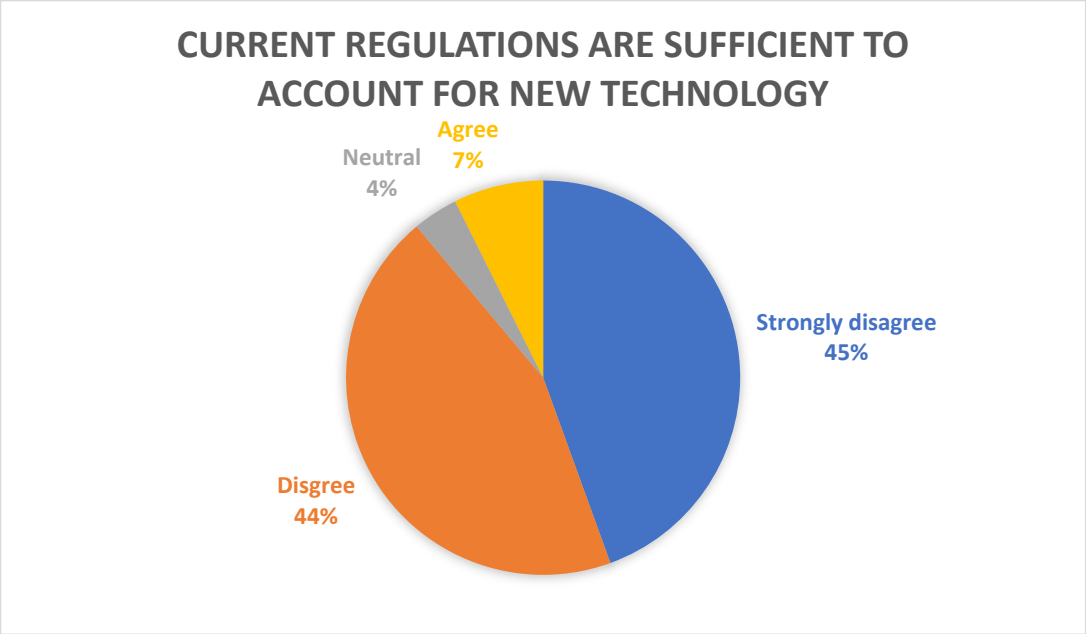

Figure 8. Survey responses to the statement "Current legal/regulatory regimes are sufficient to account for changes in new technology and will not need to be revised or reformed to adapt".

Figure 4 shows that 96% of respondents disagreed or strongly disagreed that current levels of cybersecurity in ships are sufficient to counter or defend against threats from criminal groups. In Figure 5, confirmed that awareness of attacks that have occurred on the maritime sector is high among respondents with 90% agreeing or strongly agreeing that they are aware of cyber-attacks against ships, ports and shipping companies. From Figure 6, 89% agreed or strongly agreed that criminal groups such as pirates, terrorists and transnational organised crime groups will utilise cyber and other emerging maritime technology to further their criminal enterprises. From Figure 7, there was slightly less consensus for the statement "cybersecurity in the maritime sector lags behind cybersecurity in other areas of critical infrastructure" with 15% responding neutral, however, 81% agreed or strongly agreed with the statement. Meanwhile, survey results

Regarding governance, Figure 8, (discussed in part 4 below), 89% of respondents disagreed or strongly disagreed that current legal/regulatory regimes accounting for new technology in shipping is sufficient and will not require revision or reform.

Respondents in the survey were given the option of providing further comments to each of the statements and a number of key, illuminating comments are provided in full in italics with analysis below:

- *The crucial question is not the systems on board but the level of interfaces ship to shore and vice versa.*
- *Increasing reliance on these new technologies and loss of institutional knowledge of how to operate without them is a risk.*
- *Most of these systems are technically vulnerable and have been found to be compromised for years.*
- *These systems provide a false sense of security for the mariner.*
- *It would be necessary also to implement software quality assurance (SQA) in shipping. Many systems do not work because of software problems and not of cyber-attack.*
- *What regulations? It's still the wild Wild West.*
- *Mandate cyber-security training as part of STCW and the various model courses associated with port security. Add security and specifically cyber security to the areas included in the IMSAS Audit scheme.*
- *Certainly more study groups are required and international agreement on national policies because IMO cannot do it all...*

Several of these points were confirmed in interviews providing further support for the conclusions that:

a) Traditionally ships with highly intermittent satellite internet connections provided relative isolation and security for outdated and unpatched IT systems. However, this is changing with the advent of LEO satellite providers. The point was reiterated in interview with a representative of the UK Chamber of Shipping who commented "Starlink is a game changer it's now so cheap that there's all sorts of stuff going on that wasn't before in terms of remote connectivity, bandwidth" [41]. And a maritime cyber practitioner commenting:

The big thing was that ships traditionally were always standalone environments…We are now into the realms of being connected. And by virtue of the fact of the way the internet and network connectivity works, there is the ability to be seen. So the last 10 years has been a wakeup call… We have a disconnect between the real world and the maritime world. We we're now using equipment that could be on there for 10 years and would be obsolete within one. [42]

LEO always-on internet connections are highly desirable for ships' crews seeking entertainment and connectivity, however, it drastically increases the attack surface for remote cyberattack especially on outdated and unpatched IT systems. This is exacerbated by 'just-in-time' approaches to shipping which minimise time spent in ports but maximise the difficulty of patching and updating hardware and software, and further exacerbated by budgetary constraints from ship owners reluctant to invest in updating hardware and software.

b) Whereas this article will not discuss emerging technology such as autonomous vessels, discussed at length elsewhere [15,16,43], there is broad consensus that a convergence of IT and OT systems is occurring. Also, that crews are increasingly reliant on sophisticated interconnected bridge systems for navigation and monitoring of critical systems; and, while there is awareness of attacks on the maritime sector at a management/strategic level, there is a lack of preparedness or maturity with regard to cyber hygiene and cybersecurity among "understaffed and overworked" [44,45] ships' crews, who see their primary function as sailing the ship. Further, some software systems may be prone to failure without cyberattack. This reinforces the conclusion that crews may not be aware in many cases when a cyber-attack is occurring and underlines the need for training and simulations of cyber-attacks on ships.

c) An "increasing reliance" on digital systems, a "loss of institutional knowledge of how to operate without them" and "a false sense of security for the mariner" all contribute to the conclusion that to cause a catastrophic incident in shipping, in particular in a highly congested shipping lane, is confusion. As commented by a Professor of maritime cybersecurity:

You don't actually have to cause a ship to have an accident. You just need to confuse the crew…around 80% of maritime accidents are human error…you just need to bring on that human error…this can be done through false or spoofed AIS or GPS signals, you just need two conflicting sources of information to cause confusion… another thing is younger crews tend to be very focused on the technology on the bridge. And this is something we've observed in simulations. They're all looking down. Whilst, traditionally mariners, they look out, they're looking at the real world. [29]

These comments underline common themes from interviews that there is a need for simulation-based training to prepare crews for both malfunctions of IT and OT systems and cyber attacks, and the ability to tell when a cyber attack has occurred. It also underscores the need for redundant systems, and triangulation and cross-checking of data from multiple independent sources.

3. Threat Actors in the SOMS

3.1. Terrorism

Having discussed the nature of cyber and hybrid threats to the MTS in the preceding section, this section will focus on a specific geographic zone (the SOMS) to present an analysis of the likely non-state threat actors[4] and their motivations and vectors for targeting international shipping.

Taking account of past incidents and capabilities of malicious actors in and around the SOMS, how likely is it that they could conduct kinetic, cyber or cyber-physical attacks on shipping?

[4] This article does not include discussion of threats to shipping from state actors.

Interviews indicate that Indonesian terrorist groups – the country with the most active terror networks and cells in the SOMS littoral states – have some level of skill in using online tools for recruitment and financing, however, are unlikely to have the necessary knowledge or background in conducting attacks on the maritime sector. Whereas, "the maritime terrorism threat is largely a Southern Philippines phenomenon" and proven links exist between regional groups in Philippines, and the SOMS littorals [46]. Indonesian terrorist groups Jemaah Islamiyah (JI), Jemaah Anshorut Daulah (JAD) and others have targeted the maritime domain in the past. In 2005, JI planned a USS Cole-style attack on shipping in the Sembawang region of the Johor strait separating Singapore from Malaysia in a "strategic kill zone where…a warship would not have room to avoid a collision with an explosive-filled suicide boat" [47].

An advanced plot in August 2016 by an Indonesian group linked to ISIS, *Katibah Gonggong Rebus* (KGR) led by Gigih Rahmat Dewa planned to shoot a rocket from the Indonesian island of Batam, across the Singapore Strait to strike the landmark Marina Bay Sands (MBS) resort [48]. One of Bahrun Naim's protégés, Dodi Suridi, "had been able—based on information gleaned from YouTube—to build and successfully test-fire a makeshift rocket launcher employing a plastic tube, potassium nitrate extracted from fertilizer, and other substances" [48]. In February 2004, the Philippines-based Abu Sayyaf Group (ASG) committed its most lethal attack, a striking example of maritime terrorism, the attack on *SuperFerry 14* in Manila Harbour which killed 116 and wounded many others. The attack was far more lethal than other frequently-cited maritime terrorist attacks such as the *USS Cole* in 2000, which killed 17 US sailors and severely damaged the ship; and the 2002 attack on the *M/V Limburg*, a tanker chartered to Malaysian state-petroleum agency, Petronas, which "blew a gaping hole in the side of the tanker" [49] off the coast of Yemen killing one crew member and causing a massive and disruptive oil spill; and the hijacking of cruise ship *Achille Lauro* in 1985 resulting in one fatality [50].

From the foregoing discussion of regional terrorist threats to shipping several points are evident.

First, it is difficult to avoid the conclusion that if any of the aforementioned terror attacks had been successfully committed in or around the SOMS they would have severely impacted the flow of shipping through the region causing knock-on effects similar to that of the 2021 *M/V Ever Given* incident. The scope and scale of the disruption would depend on the incident and there have been attempts to estimate the economic disruption from such attacks [23].

Second, these examples illustrate the desire to target the maritime space and that, if the opportunity presented itself to commit a large-scale cyber-attack on shipping, it would be strongly in line with the general call to jihad that is characteristic of regional terror groups.

As a professor of regional security commented in interview:

ISIS and Al Qaeda, they make general calls to carry out operations wherever you are. The general idea is, if you cannot make *hijrah* or migration to a land of active jihad, you can carry out your jihad right where you are. I mean, your enemy is on your right and on your left, and you can carry out jihad through various means. The main thing they usually call for is outright violence, using knives, using vehicles, using fire. So it's about do-it-yourself jihadism in terms of the weaponising of everyday items. We do know that in other parts of the world, ISIS has had very capable cyber militants, for example, Junaid Hussein… I haven't seen any specific call for using cyberattacks… but in principle, I wouldn't see why not. Why wouldn't they want to do that? In principle, I believe that they would definitely be very much in favour of it, if anybody, any brother, has the ability to carry out a cyber-attack, I think they would be all for it.[46]

Such a cyber-based attack, whether on the maritime domain or on land, would be very much in line with the general call to terrorist followers to commit attacks of any kind, using whatever resources are available to hand.

Third, while a catastrophic cyber-attack on shipping has yet to be seen, it does not preclude the possibility of a "black swan event", nor that regional groups are not developing the necessary cyber skills. The advent of generative artificial intelligence that is able to create computer code compounds the likelihood of malicious groups using cyber attacks as outlined in reports from the UK's Turing Institute and EUROPOL [51,52]. Also, events in other parts of the globe, such as increased attacks on

 doi:10.20944/preprints202401.1609.v1

shipping in the Bab el-Mandeb strait committed by Houthi groups in response to violence against fellow Muslims in Gaza [1,53] influence events in Southeast Asia.

On this point, a representative of Indonesia's National Counter-terrorism Agency (BNPT) intelligence division commented in interview:

The threat of terrorism in Indonesia cannot be separated from the global situation. Whatever happens in the global terrorism situation, will have an impact on network movements in Asia and in Southeast Asia in particular. Then from talking to them they've experienced a shift to the online space, so that previously all terrorist activities were done conventionally or physically. They've also moved from physical space to cyber space. Like starting from recruitment, propaganda, military training and training to make explosives, and the provision of logistics. Then planning attacks also and up to hiding their funding. All the activities that were done in a conventional way are now done in cyberspace. They use it a lot for propaganda, glorification of all their activities they do it in the cyberspace. [54]

Finally, a cyber-attack on shipping in the SOMS would not necessarily originate in the adjacent littorals, rather, depending on the nature of the attack, could be conducted remotely from any part of the world. An attack that was hybrid in nature would likely require some kind of physical presence in the region – to covertly install malware on a ship's bridge using a USB drive for example [22].

3.2. Piracy and Other Crime

Like terrorism, the threat of piracy in Southeast Asia continues to be of concern. Data from the ReCAAP Information Sharing Centre (ISC) shows the total number of piracy and armed robbery against ships (ARAS) incidents hovering in the range of 70 – 100 incidents per year for the five years 2017 to 2022 [55].

At time of writing, data from January – June 2023 showed 59 incidents, "this accounts for a 40% increase of incidents compared to 42 incidents reported during January-June 2022"[56] making it likely the total number for 2023 will increase from 2022 but remain in the same range of 70-100. The report further notes:

The increase of incidents during January-June 2023 occurred in the Philippines, Straits of Malacca and Singapore (SOMS), Thailand and Vietnam. Of concern was the continued occurrence of incidents in the SOMS, with 41 incidents reported compared to 27 incidents during the same period in 2022.

It can be noted that all of the incidents occurred while vessels were underway, and in the majority of cases (61%) the perpetrators were unarmed, and did not harm crew (90%). Those that did carry weapons most commonly used knives and machetes. Only one report in 2022 noted perpetrators carrying guns. In two incidents crew were taken hostage but were able to escape, and in two other cases crew were assaulted. Items stolen were ship's property, engine spares, and unsecured items. This picture largely confirms the comments of one Indonesian Coast Guard source who stated in interview:

These incidents are not piracy, they are more like petty theft, petty crime. It's also not uncommon that the crew themselves steal the items and report it as being stolen.

And further:

The information from the IMB and the IFC is often not accurate. We want to give seafarers a correct picture that's we why we set up the Indonesia Maritime Information Centre (IMIC). [57]

A monthly report from the IMIC for June 2023 records a number of different maritime incidents including drug trafficking, IUU fishing, irregular human migration and maritime accidents, but does not record any piracy or ARAS incidents for the period. It does include a category for 'petty theft' [58].

Head of the Indonesian Maritime Institute when asked about piracy in the SOMS commented:

The Singapore Strait is very busy, so the vessel must be in low speed. So it is very attractive for these guys to onboard your vessels. They take laptops, watches and then fly back to their boat. This is not piracy. But is sometimes reported as piracy to hurt Indonesia's feelings. It's spontaneous and not well organized. There is another type which has international connections that target tankers.

 doi:10.20944/preprints202401.1609.v1

This is not locals, this is beyond their capacity. To hijack tankers and extract the fuel is a tricky business. This is very rare in Indonesia and always involves international actors. The bosses are in Singapore, and the operators are in Batam.

While the levels of piracy in and around the SOMS remain at a level that would be of concern to any reasonable captain transiting the straits, it may be said that they are largely of a type that is opportunistic petty theft while underway, than acts of extreme violence. However, occasional acts of assault and hostage-taking still occur. Regardless, it may be observed that in all cases the goal of pirates and armed robbers is not to block traffic in the strait; indeed they profit from increased traffic as it enlarges the number of their potential targets. While ReCAAP issues regular advice and updates to captains of ships transiting the SOMS; if levels of piracy and crime were to significantly increase in frequency and violence it could severely disrupt shipping through the straits. At present this is not the case. Indeed one

Singaporean academic and expert in regional maritime security pointed out that the targets of piracy in the SOMS are, in a majority of cases, vessels plying regional routes rather than ultra large international tankers and cargo ships stating "when we look at maritime crimes and the victims, the victims are usually those plying regional routes only, not those of international trade… if you go through the last 20 years data, most of them are interregional or going between Indonesian ports" [59]. These are the so-called 'rust buckets', very small tankers, and small general cargo vessels that are 'low and slow' and present the easiest targets to board while underway. "When you read headlines like 'Tanker Hijacked in the Strait of Malacca' look into the detail of how big the tanker is" she advises [59]. However, the motivation for targeting interregional shipping is due to the vulnerability of the 'low and slow' targets. If regional pirate groups discovered an easy method of remotely disabling a larger international tanker or cargo ship, they may be bold enough to attempt to exploit it. Although any attempt to target international shipping, and the subsequent media attention it would generate, would certainly lead to a response from the authorities in the littoral states, likely coordinated under the auspices of ASEAN, and executed under the framework of the Malacca Straits Patrols [60] (MSP) a regional grouping tasked with securing the SOMS.

Statistics issued by ReCAAP show that there were two violent crew abduction incidents (Category 1 incidents) per year in 2018 and 2019, and a single incident in 2020. The ReCAAP At time of writing the most recent ReCAAP quarterly report states "There was no report of incident of abduction of crew for ransom during January-September 2023. The last known incident occurred on 17 Jan 2020. No crew is currently held in captivity by the ASG. The Philippines, Malaysian and Indonesian authorities continued to maintain surveillance and military operations to neutralise the ASG." [55] However, ReCAAP advises "with the presence of the remnants of the ASG in the area, the threat of abduction of crew for ransom in Sulu and TawiTawi continues to remain" [56].

Particularly relevant to this discussion of maritime cybersecurity, is the use of technology employed in piracy and robbery. In one notable case criminals hacked into the shore side computer systems of a shipping company to identify high value cargo. While the ship was transiting the SOMS pirates boarded, armed with barcode readers, proceeded to scan containers looking for the particular cargo they wanted, in this case jewels, forced open the container stole the cargo and made their escape. It is a good example of a criminal enterprise using digital technology to augment their attacks on shipping [5]. It is difficult to gauge to what extent pirate groups are using cyber capabilities. The ReCAAP ISC report which catalogues and dissects multiple aspects of the recorded cases from the time of day of the attack, to the size of the group, the weapons they carried, etc, makes no mention of 'cyber' aspects in any of the cases presented. [56].

4. Governance

Discussions around cybersecurity vulnerabilities in ships, and the likelihood of them being exploited by malicious actors, prompts a discussion around what is being done in terms of regulation to address the challenge and shore up vulnerabilities. In this regard there are a number of developments that can be pointed to, however, the challenge of raising the bar of maritime cybersecurity in the real world remains significant as discussed below.

4.1. International governance of cybersecurity in ships

In 2017, the IMO Maritime Safety Committee (MSC) issued *Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems*.[61] This was the first attempt of the international governing body to address maritime cybersecurity in a formal way. It is a brief one-page document which issues "high level guidance" under the framework of the International Safety Management (ISM) Code, affirming that cyber risk management should be taken into account as part of a ship's overall safety management systems. It also "encourages" administrations to ensure that cyber risks are "appropriately addressed in safety management systems" no later than the ship's first annual inspection of documents after January 2021.[61] In June 2022, the IMO Facilitation (FAL) Committee issued MSC-FAL.1-Circ.3 *Guidelines on Maritime Cyber Risk Management*, again a brief document at four pages but which provides further guidance insofar as it lists potential vulnerable systems, specifically identifies that a "distinction between information technology and operational technology" should be considered, identifies malware, outdated software, weak passwords, network segregation, ineffectual firewalls, and others as vulnerabilities that can be exploited. The circular identifies five "functional elements" of cybersecurity, and directs users to further guidance from shipping organisations like BIMCO, the International Standards Organization (ISO), International Electrotechnical Commission (IEC) and the NIST framework.

Key to understanding the impact of these regulations is paragraph 2.2.2 which states:

Recognizing that no two organizations in the shipping industry are the same, these Guidelines are expressed in broad terms in order to have a widespread application. Ships with limited cyber-related systems may find a simple application of these Guidelines to be sufficient; however, ships with complex cyber-related systems may require a greater level of care and should seek additional resources through reputable industry and Government partners.[62]

As one source confirmed in interview:

This is very high level signpost guidance. And one of the reasons it was done in that way is because there's a huge amount of guidance out there that's been developed by industry and various national governments. So it was felt that we provide the high level guidance and of course it is up to member states then to read through the detailed guidance and adopt what they want to, to implement effective cybersecurity.[63]

These passages underline two important aspects of international maritime cyber regulation: first, some flexibility is needed as not all ships (or shipping companies) are the same. Second, states members will implement these requirements in their own way, according to their own needs and practices.

In practice, in most jurisdictions this means that ships, and ports, must be able to show that cyber risk has been included as part of an overall risk assessment, and that a minimum level of cyber security is in place. As MSC 428(98) points out, as part of the ship's safety inspection and documentation, cybersecurity must be included in the risk management plan – to some extent. Classification Societies, which have the task of certifying ship safety must incorporate cyber risk into their inspections. As a representative of the Dutch Ship-owners association put it when asked about cybersecurity regulation in ships:

There are guidelines, but straight forward rules about how to implement cyber security are actually not there. It's like you need to be aware, you need to have thought through all the elements on board where your risks are and you need to have written it down in your SMS [Safety Management System]. How you handle them, what your judgment is on those risks, but there's no regulations, as such.[64]

In the UK for example, pursuant to *The Merchant Shipping (Recognised Organisations) (Amendment) (EU Exit) Regulations 2019* [65], six registered organisations (ROs) including Lloyd's Register, American Bureau of Shipping and others, are authorized to conduct surveys and inspections of ships on behalf of the Maritime and Coastguard Agency (MCA). Where an RO is not satisfied that cybersecurity has been sufficiently covered it could deny issuing the Safety Management System certificate and the ship will be prevented from sailing until the deficiency is rectified.

In June 2023, the IMO announced that the cybersecurity circulars will be undergoing a comprehensive revision. The revision will be led by member states who will present a proposal to the MSC and it is too early to tell to what degree of specificity the revisions will go, or when it will be complete. At a minimum the revision will update the links to the industry guidelines to make sure they are updated to the latest versions available. It should be noted that the idea of "a standalone Cyber Code" has been raised "based on a framework created by previous IMO Codes such as the Polar Code. Since the IMO uses Codes as a legally binding instrument, this would help to ensure the continued safety and efficiency of the maritime industry in the face of threats from cyberspace" [66]. As the IMO works on the consensus of member states this would be a highly ambitious project – and would take years to complete – but ultimately could be an effective way of combining all cyber regulations and requirements into one instrument.

4.2. ISPS Code

Created in the post-9/11 years, the International Ship and Port Security Code (ISPS) focusses on the prevention of a terrorist attack against shipping. Enacted under SOLAS chapter XI-2, on 1 July 2004 the ISPS provides a comprehensive framework for the security of ports and ships, including mandatory (Part A) and recommendatory (Part B) provisions. As one EU-based legal expert interviewee noted, the ISPS was primarily concerned with physical security, however, there has been discussion in recent years about whether it also applies to digital security.

The European Union did pick up ISPS as a whole and translated it into European law and that had to be picked up by Member States and had to be implemented into the various national legislations in Europe. We sought a robust answer of whether digital security is part of ISPS. There was some nervousness about whether it was or not, if it was not it could require new legislation, and that might not come or it could take a long time. So everybody now takes the stance, 'yes' it is in ISPS and we hope that if there is a case before a court and a judge has to give an opinion, an interpretation, he or she will come to the conclusion, 'yes, digital security is also part of ISPS'.[67]

The ISPS was clearly not written to give detailed guidance on cybersecurity. The words 'cyber' or 'digital' do not appear in the document. However, as the ISPS is written in fairly broad terms, and the spirit of the document is clear (that is, to comprehensively assess security vulnerabilities and create plans to address them), it is possible to imply its mandatory application to cyber systems. For example 8.4.3 the Ship Security Assessment, mandates "identification of possible threats to the key ship board operations". Taking account of technological developments in shipping since 2004, this surely must include cyber threats. Indeed in Part B, the recommendatory provisions specifically include computer networks. Part B Section 8 Ship Security Assessment (SSA), article 8.3.5 states "radio and telecommunication systems, including computer systems and networks" should be addressed in the SSA among other essential systems. Likewise the Port Facility Security Assessment (PFSA) provisions include at 15.3.5 "computer systems and networks" in the same way. It is reasonable therefore to conclude that the ISPS does require security assessments to include cyber systems and this appears to be the approach in the EU however a test case has not yet confirmed the point.

4.3. International Association of Classification Societies (IACS)

In April 2022, the International Association of Classification Societies (IACS) issued Unified Requirements (UR) *E26—Cyber Resilience of Ships*[68] and *E27—Cyber Resilience of On-board Systems and Equipment* [69]. The purpose of the URs is to "provide a minimum set of requirements" for cyber resilience of "the ship as a collective entity" (E26) and for "on-board systems and equipment" (E27). At 32 (E26) and 14 (E27) pages respectively the URs provide much more detailed guidance than the IMO Circulars or the ISPS, covering specific aspects of cyber security like firewalls, segregation, air gapping, data diodes, and maps out Sub-goals for each functional element: identify, protect, detect, respond, recover. Both URs note that they are "to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1 January 2024 and may be used for other ships as non-mandatory guidance." [68] Implementation of the two UR's was subsequently postponed until 1 July

 doi:10.20944/preprints202401.1609.v1

2024, and they have undergone "extensive changes" including dividing the requirements into mandatory and non-mandatory depending on the size and type of ship [70].

Implementing the UR's in practice may present a challenge for ship owners particularly smaller operators with limited cyber knowledge as expressed by one interviewee:

You get a new system from a supplier and it's put on board and then you need to make sure that it becomes cyber secure when it's connected to all the other systems on board. That's an issue especially on older ships where many ship owners do not exactly know how to handle that and because they do not have the knowledge about that system and about the technical aspects of the other systems and how they can make them cyber secure.[64]

It should be clarified here that the mandatory aspects of UR E26 and E27 only apply to new build ships, and as such will not cause regulatory deficiencies in existing ships. However, they provide a useful guide of where maritime cybersecurity regulation is heading; that is, a requirement that Original Equipment Manufacturers (OEMs) provide devices where cybersecurity is an inherent aspect of their design, and that, when installed alongside other ship systems, the cybersecurity of the *whole* is assured.

4.4. Port State Controls

Port State Controls (PSCs) are an important element in enforcing safety in shipping, and they will play an important role in maritime cybersecurity. As a representative the Netherlands ship-owners association informed "we have members who have gone to the US for example who tell us that they have been questioned for two hours about their cybersecurity on arrival in the port. In other countries it might be quite basic. You have the port state control system and then you have all kinds of reasons for a deficiency, but there's not a specific rule for cyber security." [64] Some port states are clearly implementing stringent inspections on cybersecurity. However, to date it does not appear that there has been a detention based on a cybersecurity deficiency. For a Port State Control Officer (PSCO) to detain a ship requires "clear grounds" of a breach. For physical systems like fire safety, or lifeboats, where clear requirements are set out, this is much easier to prove or show with photographic evidence for example. Ship cybersecurity breaches are much more difficult to prove, and the regulations and overall expertise from both sides, the inspection side and the ship operator side is not yet sufficient. A PSCO who detained a ship based on alleged cybersecurity defects would be at risk of legal challenge by the ships owners and the possibility of liability for losses arising from the ship's detention [67]. For that reason, it is unlikely that ship detentions will occur as part of PSC unless there is very clear evidence of a deficiency. Further, a detention would seem unlikely until there are clearer practical guidelines on what exactly would constitute clear grounds of a cyber deficiency.

4.5. Maritime Single Window

The Maritime Single Window (MSW) is an IMO initiative to streamline ship documentation processes when coming into port, whereby all documentation will be submitted online through a single portal. Whereas Safety Certificates are among the bundle of documents required – including passenger lists, pre-arrival security form listing previous ports of call and others – there is no current requirement for a specific cyber security, or cyber qualification certificate as part of that bundle. As one interviewee noted "there is no specific form to say that the ship is cyber secure. That's not one of the existing file forms. And as mentioned, there's no plan in the short term at least to introduce such a form. But what we do have is the MSC resolution." [63] As noted above, if the ship does not have a valid ship safety assessment and plan, issued by their Class Society, which should incorporate cyber security this would be grounds for detention. At time of writing, there is an initiative to require "systematic and mandatory attention for cybersecurity" as part of the implementation of the MSW [67]. This could be achieved through the regular Amendments to FAL (the Annex to the Convention on Facilitation of International Maritime Traffic, 1965 (FAL Convention)) by inserting into Section 1 C. Systems for the electronic exchange of information a new Paragraph:

 doi:10.20944/preprints202401.1609.v1

1.4 Cybersecurity – Contracting Governments shall safeguard the cybersecurity of entities operating and being connected to the system for the electronic exchange of Information by creating a mandatory framework. [67]

As the MSW will require a centralisation and digitalisation of documentation for ships entering and departing international ports, it would seem a pertinent requirement for national governments of port operators to incorporate cybersecurity into the designs, frameworks, portals and online infrastructure of such processes, in much the same way as the IACS UR E26 and 27 do for shipboard devices and systems.

4.6. Regional governance of threats to maritime security

A detailed discussion of the domestic approaches of each of the littoral states to maritime security and cybersecurity is beyond the scope of this paper. Instead this section discusses the regional cooperative efforts to secure shipping through the SOMS and some major developments in the governance structures of the littorals.

Significant progress in regional cooperative measures for maritime security has been made in the past two decades, since the Malacca Strait Patrols (MSP, originally named MALSINDO) began operations in 2004 [71]. The MSP entails coordinated naval patrols, Eyes in the Sky (EiS) aerial surveillance, and intelligence exchange and sharing. This collective approach to maritime security was praised in 2008 by then-IMO Secretary-General Efthimios Mitropoulos as "a model to emulate in addressing the Gulf of Aden piracy problems. This accolade was also echoed by the US Pacific Command in 2012" [71].

In 2022, Indonesia's foreign minister Retno Marsudi stressed the need to enhance maritime cooperation through the ASEAN Maritime Outlook [60]. Indonesia has also been instrumental in driving the ASEAN Coast Guard Forum [72].

Indonesia, often criticised for a lack of inter-agency coordination and cooperation between its maritime security authorities, is in the process of revising the legal basis of its Coast Guard agencies, that is Badan Keamanan Laut (BAKAMLA) and the KPLP [73]. The current administration supports a revision to Law Number 32 of 2014 on Maritime Affairs which would make the KPLP subordinate to Bakamla and consolidate the position of Bakamla as the lead agency for maritime security [73].

There is currently no regional framework to specifically address maritime cybersecurity, however, multiple sources confirmed in interview that cybersecurity has received considerable attention from the government agencies mentioned above in the three littoral states. The Indonesian Coast Guard (Bakamla) for example confirmed in interview that "in 2021 cybersecurity was added to the nine threat types that we focus on" and further the intention to strengthen regional cooperation through the ASEAN Coast Guard Forum which was seen as a truly regional initiative [57].

5. Conclusion and Recommendations

The preceding analysis, drawing on primary data from surveys, interviews, roundtable discussions, conference papers, reports, and insights from the Maritime Cybersecurity Database, yields critical conclusions and recommendations for the maritime sector's cybersecurity landscape.

Firstly, it is evident that cybersecurity attacks on the maritime industry are on the rise, evolving in sophistication, with a noticeable increase in ransomware payments. This escalating threat is exacerbated by challenges such as aging, outdated, and unpatched IT systems on ships, the growing connectivity from Low Earth Orbit (LEO) satellite internet, the convergence of IT and Operational Technology (OT) systems, and a deficiency in cyber awareness and hygiene among ships' crews. The shortage of IT and cybersecurity staff onboard further compounds these vulnerabilities. Data from surveys and interviews confirms a number of points in regard to cybersecurity in the maritime sector, in brief: an increasing reliance on ICT and networked devices in shipping creates challenges for traditional ship's crews; current levels of cybersecurity in ships are insufficient, as are current regulations, and criminal groups will leverage cyber vectors and new technology to pursue innovative ways of conducting their illicit activities.

Addressing these issues requires a multifaceted approach. One key recommendation is the imperative need for comprehensive cybersecurity training and simulations to enhance preparedness and awareness among ships' crews. This becomes particularly crucial in light of the potential for catastrophic accidents, especially in congested shipping lanes such as the Strait of Malacca and Singapore (SOMS). The injection of confusion into a ship's bridge could lead to collisions or accidents, underscoring the urgency of heightened preparedness.

In the SOMS region, the looming threat of terrorist actors targeting shipping persists, with a history of malicious attacks on critical infrastructure. While piracy remains largely opportunistic, security organizations warn of the continued possibility of violent crew abductions. In response, the maritime industry must remain vigilant and cooperative within regional frameworks like the MSP, ACG, and ASEAN Maritime Outlook.

On the regulatory front, progress is being made with initiatives like the International Maritime Organization's (IMO) circulars, mandating cybersecurity integration into a ship's overall risk assessment processes. The International Ship and Port Facility Security (ISPS) Code and the International Association of Classification Societies (IACS) Universal Requirements (UR E26 and E27) are pushing for mandatory cybersecurity in device design, albeit with a realization that enforcement, and real-world results, will take time. Nevertheless the regulations highlight cybersecurity as an aspect of ship design, and the important point that a device is only as secure as the systems that it is connected to.

However, challenges persist in the practical implementation of regulations. Port state controls, while demanding clear evidence of a cyber breach, lack practical guidelines for Port State Control Officers (PSCOs). The beginnings of PSCs in some jurisdictions, such as questioning ship masters about shipboard cybersecurity during port visits, can be seen and will raise industry awareness. Still, PSC detentions on cybersecurity grounds are unlikely in the near term due to a lack of clarity on breach definitions and concerns about liability.

To fortify the maritime cybersecurity ecosystem, enhanced cooperation and coordination among domestic governmental agencies in the SOMS littorals are imperative. Information sharing of cyber threat intelligence should be prioritized, and the establishment of a non-mandatory, anonymous reporting framework is crucial to fostering a proactive and collaborative response to emerging threats.

While a catastrophic, cascading cyber attack on a shipping chokepoint like the SOMS has not occurred, laboratory tests have proven the potential for such a "black swan" event. The serious and coordinated attention of maritime security stakeholders is required to mitigate the risks associated with disrupting multiple ships simultaneously or causing collisions in strategic shipping lanes. As the industry navigates these challenges, proactive measures, cooperative frameworks, and regulatory enhancements will be paramount in safeguarding the maritime sector against evolving cyber threats.

Funding: This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 101029232.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Ethics Committee of xxxxx , UK reference number: P136040 June 2022.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data from this study is not publicly available due to ethics requirements.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Executive, M. *MSC and CMA CGM Suspend Red Sea Transits, Joining Hapag and Maersk*. Maritime Executive, 2023.
2. Jain, A. *Suez Canal blockage by Ever Given may cost up to $1bn, say authorities*. Independent, 2021.
3. Diane Zorri, G.C.K. *Cyber Threats and Choke Points: How Adversaries are Leveraging Maritime Cyber Vulnerabilities for Advantage in Irregular Warfare - Modern War Institute*. Modern War Institute at West Point, 2021.

4. Akarca, O. *The World's Top 10 Strategic Straits and Channels*. More Than Shipping, 2019.
5. Murdock, J. *Sea pirates ditch guns for computer hacking to plunder booty from cargo ships*. International Business Times, 2016.
6. Kessler, G.C. and S.D. Shepard, *Maritime Cybersecurity: A Guide for Leaders and Managers* Second Edition ed. 2022.
7. UNCTAD, *Review of Maritime Transport Challenges faced by seafarers in view of the COVID-19 crisis* 2021, UN Conference on Trade and Development
8. Bueger, C., T. Edmunds, and R. McCabe, *Into the sea: capacity-building innovations and the maritime security challenge.* Third World Quarterly, 2020. **41**(2): p. 228-246.
9. OECD *Ocean shipping and shipbuilding - OECD*. OECD Better Policies Better Lives, 2023.
10. Höyhtyä, M., et al. *Connectivity for autonomous ships: Architecture, use cases, and research challenges*. in *2017 international conference on information and communication technology convergence (ICTC)*. 2017. IEEE.
11. Tam, K. and K. Jones, *Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping.* Journal of Cyber Policy, 2018. **3**: p. 1-18.
12. Yağdereli, E., C. Gemci, and A.Z. Aktaş, *A study on cyber-security of autonomous and unmanned vehicles.* The Journal of Defense Modeling and Simulation, 2015. **12**(4): p. 369-381.
13. Hemminghaus, C., J. Bauer, and E. Padilla, *BRAT: A BRidge Attack Tool for cyber security assessments of maritime systems.* TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 2021. **15**(1): p. 35-44.
14. Askari, H.R. and M.N. Hossain, *Towards utilizing autonomous ships: A viable advance in industry 4.0.* Journal of International Maritime Safety, Environmental Affairs, and Shipping, 2022. **6**(1): p. 39-49.
15. Fenton, A.J. and I. Chapsos, *Ships without crews: IMO and UK responses to cybersecurity, technology, law and regulation of maritime autonomous surface ships (MASS).* Frontiers in Computer Science, 2023. **5**.
16. Fenton, A.J. and I. Chapsos, *Robot Boats: Use of Autonomous 'Ships' in Law Enforcement, Terrorism and Counter-Terrorism.* Maritime Interdiction Operations Journal, 2022. **24**: p. 12-17.
17. L3HARRIS *C-WORKER 7 Autonomous Surface Vehicle (ASV) Offshore Work-Class ASV*. 2021.
18. MSubs, *Interview with representative from UK autonomous vessel manufacturer MSubs*, A. Fenton, Editor. 2022.
19. UKRN *Experts in innovation take the Royal Navy's newest vessel to sea*. Royal Navy News, 2023.
20. Palmejar, E. and N. Chubb, *The Learning Curve: The state of artificial intelligence in maritime*, T.-L.s. Register, Editor. 2023.
21. Sivori, H. and L. Brunton, *Out of the Box: Implementing autonomy and assuring artificial intelligence in the maritime industry*, T.L.s. Register, Editor. 2023, Thetius IQ.
22. Tam, K., et al., *Case study of a cyber-physical attack affecting port and ship operational safety.* Journal of Transportation Technologies, 2022. **12**: p. 1-27.
23. Qu, X. and Q. Meng, *The economic importance of the Straits of Malacca and Singapore: An extreme-scenario analysis.* Transportation Research Part E: Logistics and Transportation Review, 2012. **48**(1): p. 258-265.
24. Tam, K., et al., *Quantifying the econometric loss of a cyber-physical attack on a seaport.* 2023. **4**.
25. Weiss, J. *Was the Ever Given hacked in the Suez Canal?* Control, 2021.
26. PMA, *Marine Safety Investigation Report Grounding of MV Ever Given at Suez Canal Egypt on March 23, 2021 M/V "EVER GIVEN" IMO No. 9811000 R-026-2021-DIAM CASUALTY DATE: March 23rd, 2021*, PMA, Editor. 2023, Panama Maritime Authority.
27. Nofandi, F., et al., *Case Study of Ship Traffic Crowds in The Malacca Strait-Singapore by Using Vessel Traffic System*. IOP Conference Series: Earth and Environmental Science, 2022. **1081**(1): p. 012009.
28. NHL, *Maritime Cyber Attack Database MCAD*. 2023, NHL Stenden University of Applied Science.
29. NHL, *Interview with Professor of Maritime Cybersecurity Netherlands NHL Stenden University*, A. Fenton, Editor. 2023.
30. Kessler, G.C. *What's the worst cyber attack you can imagine striking a shipping vessel? And how can you keeo it from hitting your fleet?* Linked In 2023 May 2023; Available from: https://www.linkedin.com/posts/garykessler_askgary-what-is-the-worst-cyberattack-you-activity-7068955197598781440-UmoI/.
31. Executive, M. *Cyberattack Hits Multiple Greek Shipping Firms*. Maritime Executive, 2021.
32. Stempel, J. *Carnival is fined $5 million by New York for cybersecurity violations*. Reuters, 2022.
33. Tuffley, D. *Major cyberattack on Australian ports suggests sabotage by a 'foreign state actor'*. The Conversation, 2023.
34. Executive, M. *Cyberattack Disrupting Northern European Oil Hubs in Major Ports*. Maritime Executive, 2022.
35. Greenberg, A. *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired, 2018.
36. USCG, *Proceedings of the Marine Safety & Security Council: Uncharted Waters: Navigating the integration of autonomous vessels*, in *The Coast Guard Journal of Safety & Security at Sea*, S. Quigley, Editor. 2022, United States Coast Guard: Washington D.C.
37. Reuters *South Korea tells U.N. that North Korea GPS jamming threatens boats, planes*. Reuters, 2016.

38. Harris, M. *Phantom Warships Are Courting Chaos in Conflict Zones: The latest weapons in the global information war are fake vessels behaving badly*. Wired, 2021.
39. Sutton, H.I. *Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base*. USNI News, 2021.
40. Kenney, M. and F. Macdonald, *Shifting Tides, Rising Ransoms and Critical Decisions: progress on maritime cyber risk management and maturity*. 2023, Cyber Owl, Thetius, HFW.
41. PA, *Interview with Representative of UK Chamber of Shipping*, A. Fenton, Editor. 2023.
42. ER, *Interview with representative from Yangosat Maritime Cybersecurity practitioner*, A. Fenton, Editor. 2022.
43. Fenton, A.J. *Ukraine: how uncrewed boats are changing the way wars are fought at sea*. The Conversation, 2023.
44. Executive, M. *GAO: Understaffed, Overworked Crews Slow Down U.S. Navy Maintenance*. Maritime Executive, 2022.
45. Nautilus *Accidents and ill-health: the forgotten Covid crisis*. 2021.
46. KR, *Interview with Professor of Security Studies Singapore*, A. Fenton, Editor. 2023.
47. Farrell, R., *Maritime Terrorism: Focusing on the Probable.* Naval War College Review, 2007. **60**(3): p. 46-60.
48. Ramakrishna, K., *The Threat of Terrorism and Extremism: "A Matter of 'When', and Not 'If' "*. Southeast Asian Affairs, 2017. **2017**(1): p. 335-350.
49. Henley, J. and H. Stewart *Al-Qaida suspected in tanker explosion*. The Guardian, 2002.
50. Kuhn, K., et al., *Protective security at sea: a counter terrorism framework for cruise and passenger ships.* WMU Journal of Maritime Affairs, 2023. **22**(3): p. 345-363.
51. Ardi Janjeva, A.H., Sarah Mercer, Alexander Kasprzyk, Anna Gausen, *The Rapid Rise of Generative AI: Assessing risks to safety and security*. 2023, Centre for Emerging Technology and Security, Turing Institute.
52. EUROPOL, *ChatGPT The impact of Large Language Models on Law Enforcement*, in *Tech Watch Flash*. 2023, Europol.
53. AJ *Yemen's Houthis 'will not stop' Red Sea attacks until Israel ends Gaza war*. Al Jazeera News, 2023.
54. BNPT, *Interview with Representative of Intelligence Division of National Counter-terrorism Agency (BNPT)* A. Fenton, Editor. 2023.
55. ReCAAP, *3rd Quarter Report Piracy and Armed Robbery Against Ships in Asia* 2023, Regional Cooperation Agreement Against Piracy ReCAAP Information Sharing Centre.
56. ReCAAP, *Half Yearly Report January - June 2023 Piracy and Armed Robbery Against Ships in Asia*. 2023, Regional Cooperation Agreement Against Piracy ReCAAP Information Sharing Centre.
57. BAKAMLA, *Interview with Representatives from Badan Keamanan Laut (BAKAMLA Indonesian Coast Guard)*, A. Fenton, Editor. 2022.
58. IMIC, *Monthly Report June 2023*. 2023, Indonesia Maritime Information Centre Badan Keamanan Laut Indonesian Coast Guard.
59. JC, *Interview with Singapore academic expert in regional maritime security*, A. Fenton, Editor. 2023.
60. KEMLU *ASEAN Maritime Outlook (AMO): Indonesia's Initiative to Strengthen Comprehensive ASEAN Maritime Cooperation*. 2023.
61. IMO, *Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems* in *MSC. 428(98)*, I.M. Organization, Editor. 2017.
62. IMO, *Guidelines on Maritime Cyber Risk Management*. 2022, International Maritime Organization.
63. IMO, *Interview with representatives of IMO*, A. Fenton, Editor. 2023.
64. CB, *Interview with Representative of Dutch Shipowners Association*, A. Fenton, Editor. 2023.
65. UK, *The Merchant Shipping (Recognised Organisations) (Amendment) (EU Exit) Regulations 2019*, in *2019 No.270 Regulation 3*. 2019: UK.
66. Hopcraft, R. and K.M. Martin, *Effective maritime cybersecurity regulation - the case for a cyber code.* Journal of Indian Ocean region, 2018. **14**(3): p. 354-366.
67. Zoelen, F.V., *Cybersecurity and the Maritime Single Window (MSW, mandatory from 2024)*, in *Cyber-SHIP Lab / International Maritime Organization Annual Symposium 2023 1-2 November 2023*. 2023: IMO London.
68. IACS *E26—Cyber Resilience of Ships*. International Association of Classification Societies, 2022.
69. IACS *E27—Cyber Resilience of On-board Systems and Equipment*. International Association of Classification Societies, 2022.
70. IACS *IACS UR E26 and E27 Press Release*. 2024.
71. Collin, K.S.L., *The Malacca strait patrols: Finding common ground.* RSIS Commentary, 2016. **91**.
72. antaranews.com *Indonesia-led ASEAN Coast Guard Forum discusses protection of waters - ANTARA News*. Antara News, 2023.
73. BPHN *Pemerintah Mendukung Perubahan UU Nomor 32 Tahun 2014 tentang Kelautan*. 2023.