ROYAL AUSTRALIAN NAVY
SEA POWER
SOUNDINGS

Issue 42, 2021

The Rising Threat of Maritime Cyber-attacks: Level of Maritime Cyber-security Preparedness along the Straits of Malacca and Singapore

By Captain Marcus Neo

Captain Marcus Neo (Republic of Singapore Navy) attended the Sea Power Centre - Australia as an ASEAN Fellow.

ROYAL AUSTRALIAN NAVY
SEA POWER
SOUNDINGS

Issue 42, 2021

Issue 42, 2021

Abstract

Maritime cyber-attacks constitute an added complexity on top of traditional maritime threats such as piracy, illegal activities, maritime terrorism and accidents at sea. The global maritime sector is increasingly digitalised, automated and connected. With it comes a host of cyber threats that have in recent years risen significantly. For instance, cyber-attacks on shore-based maritime related systems have risen nine-fold in the past few years while cases of GPS and AIS spoofing have been frequently observed. Infiltrating and thereafter controlling a commercial vessel to capsize, collide or cause environmental damage are now well within the realms of possibilities.

With these developments in mind, this research highlights the realities of maritime cyber-security through recent events and case studies. In particular, this paper examines *to what extent are Singapore, Malaysia and Indonesia ready to counter the rising threat of maritime cyber-attacks in the congested Straits of Malacca and Singapore (SOMS)*.

Through the research conducted, countries along the SOMS have displayed some degree of readiness on the national and sectoral levels to examine and counter the risks of maritime cyber-attacks. Guidelines by the International Maritime Organization (IMO) also provide some degree of baseline for commercial ships although more needs to be addressed.

On the international front, the IMO's guidelines could be improved by instituting and mandating certain clauses instead of leaving them as guidance. Countries along the SOMS may also consider improving enforcement efforts to establish a baseline layer of cyber-defence for commercial vessels flagged in the region.

Systems in the general environment are seeing degrees of technology improvement and the steady introduction of encrypted GNSS signals which are less prone to spoofing. Despite these advancements, the rate of adoption is likely commensurate with the perceived risks if they are not regulated by authorities. It is therefore critical that a culture of maritime cyber-security within these organisations is as pervasive as the "surface area" of potential attacks in the maritime eco-system.

Issue 42, 2021

SECTION I

Introduction, Importance and Research Question

The global maritime sector is increasingly digitalised, automated and connected. There are new opportunities to be leveraged, although with them come a host of cyber threats that require deeper, wider and more sustained study. The maritime shipping industry is estimated by the United Nations Conference on Trade and Development (UNCTAD) to account for more than 80% of the world's trade, but only 33% of respondents in a 2020 Safety at Sea and Baltic and International Maritime Council (BIMCO) Maritime Cyber Security survey cited their organisations are employing solutions against maritime cyber-attacks. Further, close to half of respondents indicated that operations continuity plans in place were either not tested in the last 12 months or they did not know if such tests were conducted.[1] [2]

The World Economic Forum's Global Risk Report 2020 indicated cyber-attacks on maritime infrastructure to be the fifth top risk of 2020.[3] A rise in cases of Global Navigation Satellite System (GNSS) and Automatic Identification System (AIS) spoofing, and the infiltration of shipping companies' and ports' IT infrastructure, reveal a worrisome trend.[4]

Cyber-attacks on the maritime industry's Operating Technology (OT) systems[5] have similarly increased. Reportedly up nine-fold in the past three years, many of these incidents remain unreported either because organisations are unwilling to reveal cyber-security vulnerabilities or attacks were not detected.[6]

The Stuxnet incident is a landmark case on cyber-attacks on OT systems. Attackers infiltrated and took control of the mechanical operations at one of Iran's uranium enrichment facilities, resulting in the destruction of the centrifuges and in-turn delaying Iran's nuclear programme.[7] Similar types of cyber-attacks could impact ships and maritime infrastructure. Other categories of cyber incursions on maritime infrastructure include the 2017 NotPetya ransomware attack on Maersk. This incident is a notable one given the scale, economic losses and impact to global shipping networks. Following this ransomware attack, the next three largest shipping conglomerates similarly suffered from cyber-attacks of varying levels.[8]

International bodies are not oblivious to the gravity of maritime cyber-attacks. The International Maritime Organization (IMO) issued a regulation in 2017 and gave ship owners and executives until January 2021 to include cyber-risk management plans in vessels' overall safety protocols.[9]

In the US, a *National Maritime Cybersecurity Plan* was published in December 2020 as the overarching whole-of-government (WoG) initiative to integrate cyber-security and maritime security resources and stakeholders. This plan was established to "aggressively mitigate maritime cyber space threats and vulnerability". Then-President Donald Trump indicated that the document is also a "call to action for *all* nations to join them in protecting the vital maritime sector".[10]

Taken together, maritime cyber-attacks constitute an added complexity on top of traditional maritime threats such as piracy, illegal activities, maritime terrorism and accidents at sea. Realities on the ground present a strong case for research in this field. The interest and emphasis on the international stage further anchor the importance to study this emerging threat.

With these developments in mind, this research highlights the realities of maritime cyber-security through recent events and case studies. In particular, this paper examines *to what extent are Singapore, Malaysia and Indonesia ready to counter the rising threat of maritime cyber-attacks in the congested Straits of Malacca and Singapore (SOMS)*.[11] (Refer to map in Figure 1.)

Issue 42, 2021

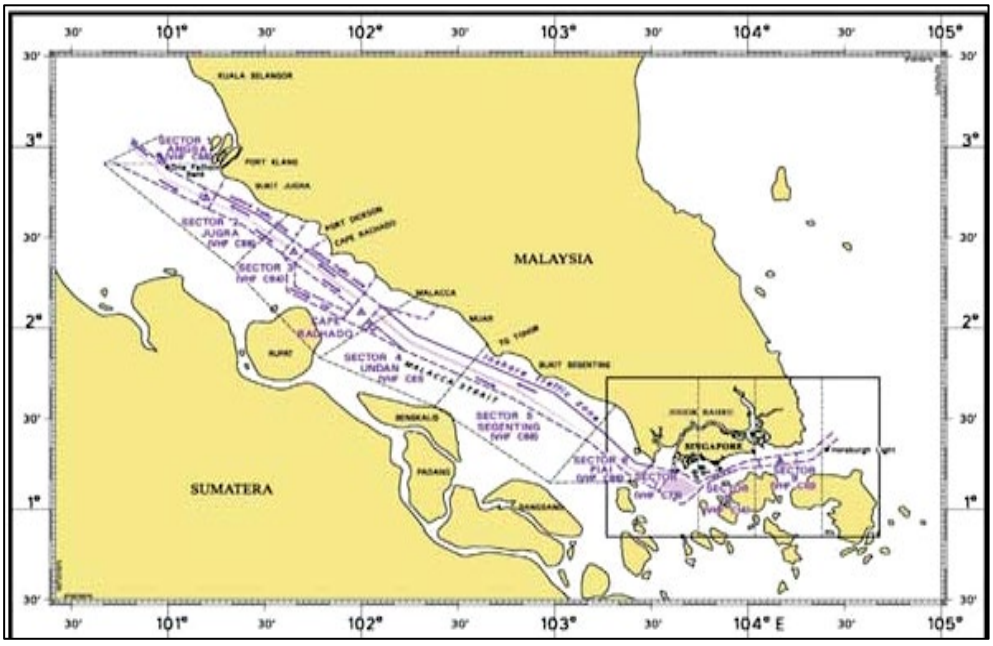


Figure 1: The Straits of Malacca and Singapore
(Source: Maritime Port Authority of Singapore)

Definition of Concepts and Terms

The following section seeks to define and elaborate on relevant concepts and terms used in the following research.

Bueger describes *maritime security* as having four primary concepts, namely (1) National Security, (2) Economic Security, (3) Human Security and (4) the Marine Environment.[12] Pertinent areas that threaten maritime security within the ambit of these four concepts include inter-state maritime disputes, maritime terrorism and illegal fishing. Hill offered a well-encompassing take where maritime security is about "creating the conditions in which peaceful use of the sea can be equitably and safely carried out".[13]

Cyber-security is defined by the International Telecommunication Union as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organisation and user's assets".[14]

According to CSO Group Australia, a *cyber-attack* is defined as an offensive launched from one or more computers against another computer, multiple computers or the networks involved. Cyber-attacks can be broken down into two broad categories: (1) Attacking with the goal of disabling target computers and/or networks or (2) Attacking with the goal of accessing and controlling computers' data and/or networks.[15] Increasingly, cyber-attacks have implications on the physical world as more Operational Technology (OT) such as cargo handling systems at ports and engine control systems onboard ships are connected to the internet. These cyber-attacks are often challenging to attribute and therefore offer actors degrees of plausible deniability.[16]

Maritime cyber-security can be defined as cyber-security in the maritime domain which involves safeguarding the sector's Critical Information Infrastructure (CII), guarding against cyber-attacks and/or other unintended errors that may disable, disrupt and/or take-control of IT and OT infrastructure.[17] These infrastructures can be divided across three areas to examine: (1) Systems in the general environment (e.g. GNSS, AIS), (2) Systems on board ships (e.g. ballast systems, propulsion control) and (3) Systems ashore (e.g. monitoring and handling systems for cargo and port operations). In the shipping insurance sector, the term coined describing maritime cyber-security of a vessel is "cyber seaworthiness".[18]

Grey zone activities are the means employed to project state power and compel outcomes while remaining within the threshold of peace.[19] Grey zone activities in the maritime domain and the use of cyber-attacks to influence geo-political outcomes have in recent years garnered significant attention.[20]

Issue 42, 2021

SECTION II

Maritime Cyber-security: Significant Cases

With the threat becoming increasingly apparent, the following section highlights significant maritime cyber-security incidents.

Systems in the General Environment

The perils of GNSS spoofing such as spoofing of civilian GPS systems is not new to maritime practitioners.[21] GNSS spoofing is the transmission of simulated false GNSS satellite ephemeris and timing information which coerces the GNSS receivers into calculating incorrect positioning. Spoofing is particularly dangerous because false signals taking over legitimate GNSS signals are designed to do so subtly and not cause alarms, unlike jamming attacks.[22]

In 2019, a British tanker *Stena Impero* was detained by Iranian forces after reportedly making a drastic manoeuvre towards Iranian waters while transiting the Strait of Hormuz. The *Stena Impero* was thought to have had her GNSS spoofed[23] which resulted in inaccurate positioning of the ship and an erroneous alteration towards Iranian territory (refer to Figure 2). As a result of this event, a civilian oil tanker became embroiled in a geopolitical fiasco[24] and saw shipping companies instructing vessels to transit the strait at high speed and only in the day.[25]

Issue 42, 2021

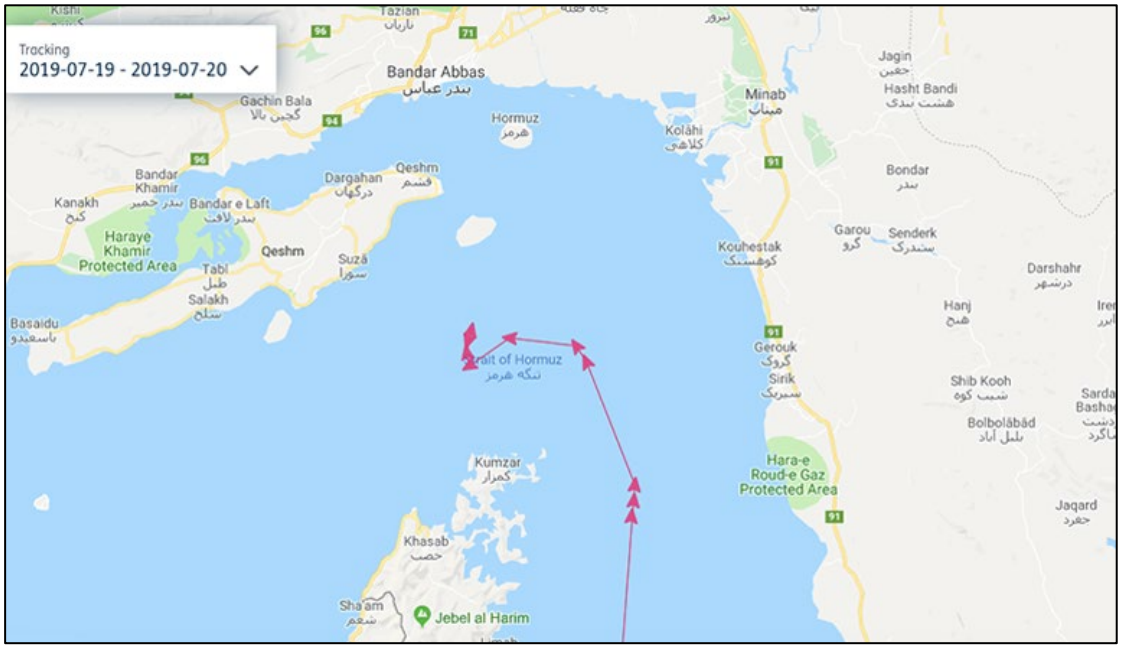


Figure 2: Stena Impero's Track and Drastic Course Alteration
(Source: Lloyd's List Intelligence)

In 2017, 20 vessels in the vicinity of the Black Sea Novorossiysk Commercial Sea Port reported a sudden and dramatic shift in their ship positions. The reported positions were 17nm inland at Geledzhik Airport, some 30nm away from the ships' actual position. This case remains unresolved although experts believe state actors were likely testing GNSS spoofing technology.[16]

AIS provides ship's position and movement information to surrounding vessels via VHF, primarily for collision avoidance. The AIS system is similarly known to have multiple vulnerabilities and one such example of AIS spoofing was detected in 2019 by the Italian Coast Guard. Following investigations by the European Maritime Safety Agency, it was revealed that an AIS signal generator spoofed AIS data and created the false readings. The analysis found 3,742 "ghost ships" created within a span of 17 minutes in a 28 × 21nm area. Monitoring of maritime traffic and discerning real versus "ghost" became impossible for maritime authorities simply because of the volume of tracks appearing on their screen[26] (refer to Figures 3 and 4).

Issue 42, 2021

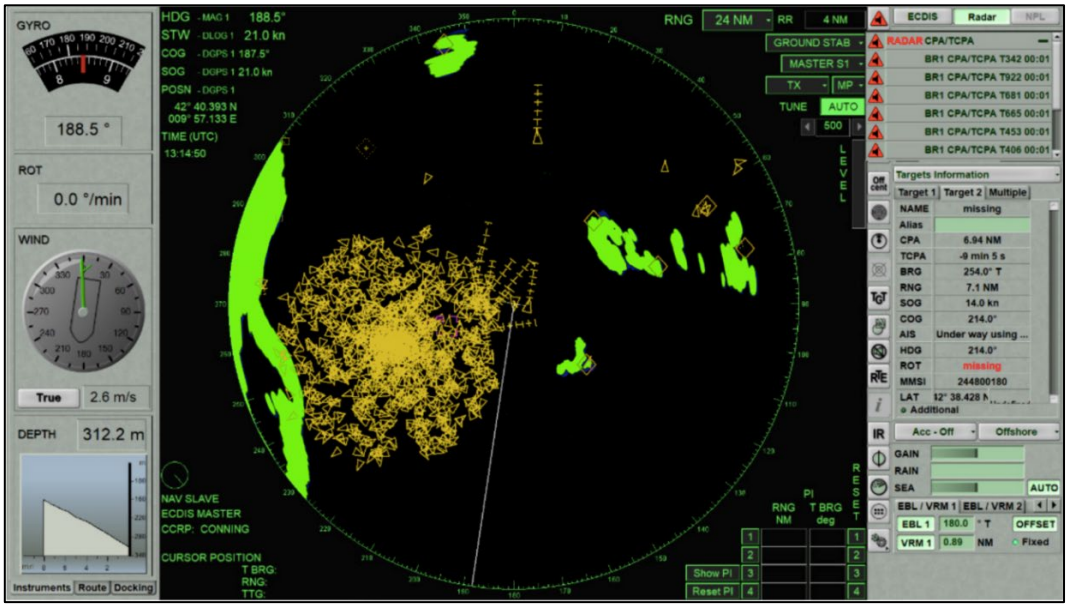


Figure 3: Radar Console with Inputs from AIS Indicating the Ghost Contacts (Source: MDPI Journal of Applied Science)

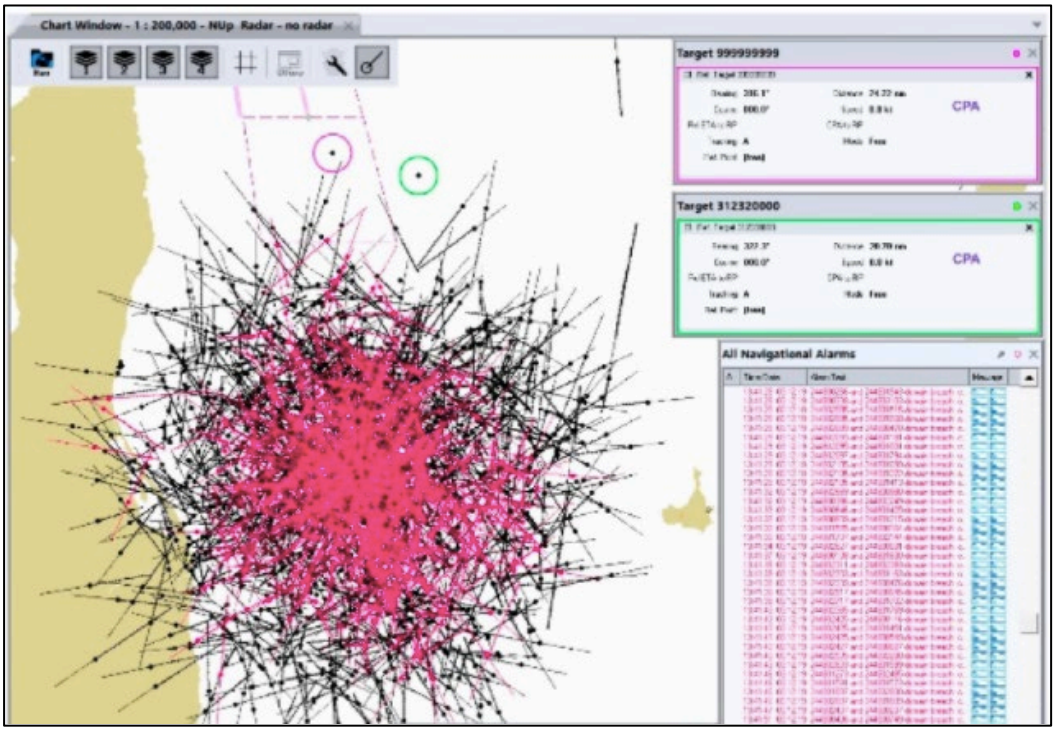


Figure 4: Vessel Traffic Service (VTS) Monitoring Console Indicating False AIS Tracks (Source: MDPI Journal of Applied Science)

AIS spoofing could also be adopted if nations are interested to mask the genuine identity of a vessel. North Korean ships are known to use "flags of convenience" on AIS to disguise the nationality of the ship in order to conduct shipping activities considered illegal under UN sanctions.[27]

Ships Systems (Maritime Operational Technologies)

Operations Technology (OT) are systems used to regulate the physical world. These systems are also commonly known as Industrial Control Systems (ICS) and include navigation systems such as the Electronic Chart Display and Information System (ECDIS), control systems for ships' ballast, engine and propulsion, and cargo management systems (refer to Figure 5). OTs are often designed to support specific capabilities onboard and are designed to be air-gapped from IT systems such as the internet-facing computers for crew use. In recent times, however, the segregation is increasingly challenged.

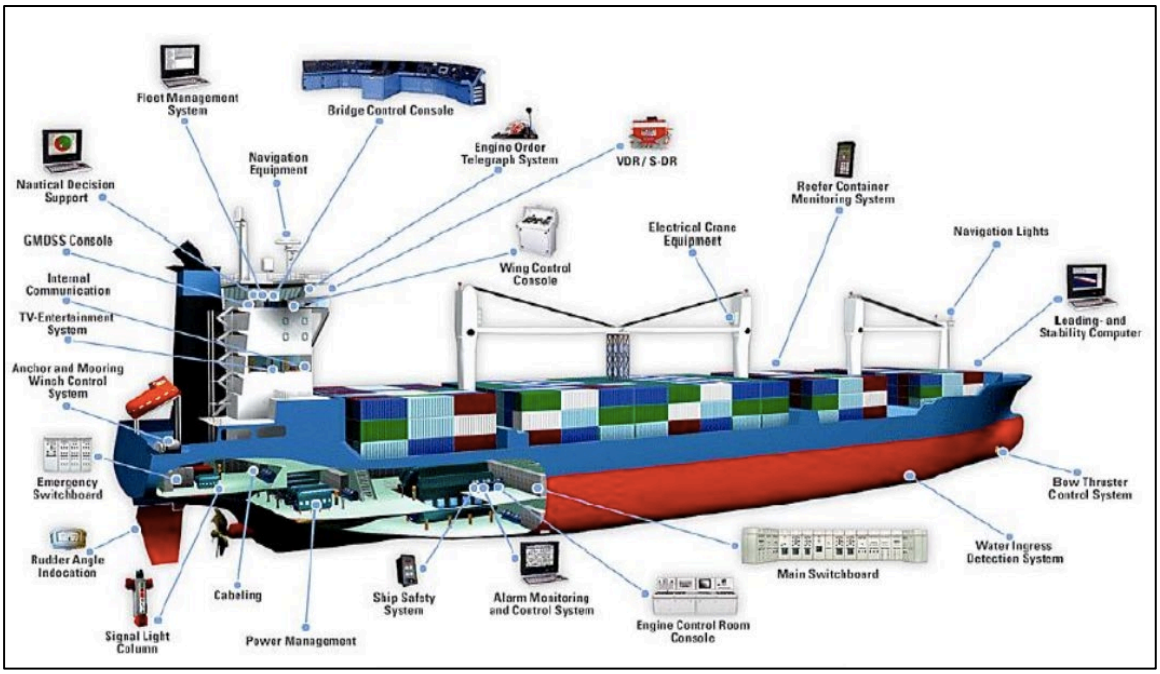


Figure 5: Electronic Systems onboard Ships
(Source: United States Coast Guard Cyber Command)

OT systems are increasingly connected to the internet for HQ's remote monitoring/access, troubleshooting, spares planning and other data analytics needs. CEO Ital Sela of cyber-security company Naval Dome[28] explained that "*COVID-19 social restrictions and border closures have further forced original equipment manufacturers (OEMs), technicians, and vendors to connect standalone systems to the internet in order to service them".*[29] *In other words, OT systems are increasingly connected to the internet which opens up more "surface area" for infiltration. A recent study conducted by KPMG revealed that 14% of respondents have critical industry OT equipment, such as Programmable Logic Controllers (PLCs), remotely accessible through the internet.*[30]

Lloyd's List and CyberCube[31] conducted a study on the emerging cyber-threat on ICS and suggested several plausible vectors of attack including (1) Third-party components compromised on the onset, (2) Command and control activation via internet-facing ICS with vulnerabilities, instigating failure in systems, (3) Physical deployment of self-spreading and pre-programmed malware directly to an air-gapped OT network by an employee either unknowingly or with nefarious intent.[32]

Although significant attacks on shipboard OT systems have not been reported, parallels cases on shore suggest that they are within the realms of possibility. An example is the prominent Stuxnet attack where attackers took control of the OT system despite it being air-gapped and conducted a gradual degradation of the nuclear centrifuges which eventually damaged them beyond repair.[33] An older case that happened in Queensland, Australia, further reinforces that such attacks and tactics, techniques and procedures (TTPs) have been around for longer than we thought.[34]

On ships, we could encounter actors manipulating engine controls to damage machineries over time or manipulating ballast pump systems and cargo-management systems to influence a ship's stability and hence its safety at port and at sea. A study was conducted on cargo-management systems and it was revealed that by infiltrating and tampering with values on the Container Load Plan while also masking electronic readings on the Hull Stress Monitoring System, actors could influence a ship's stability and, in extreme cases, cause a hull failure incident[35] (refer to Figure 6).

Issue 42, 2021

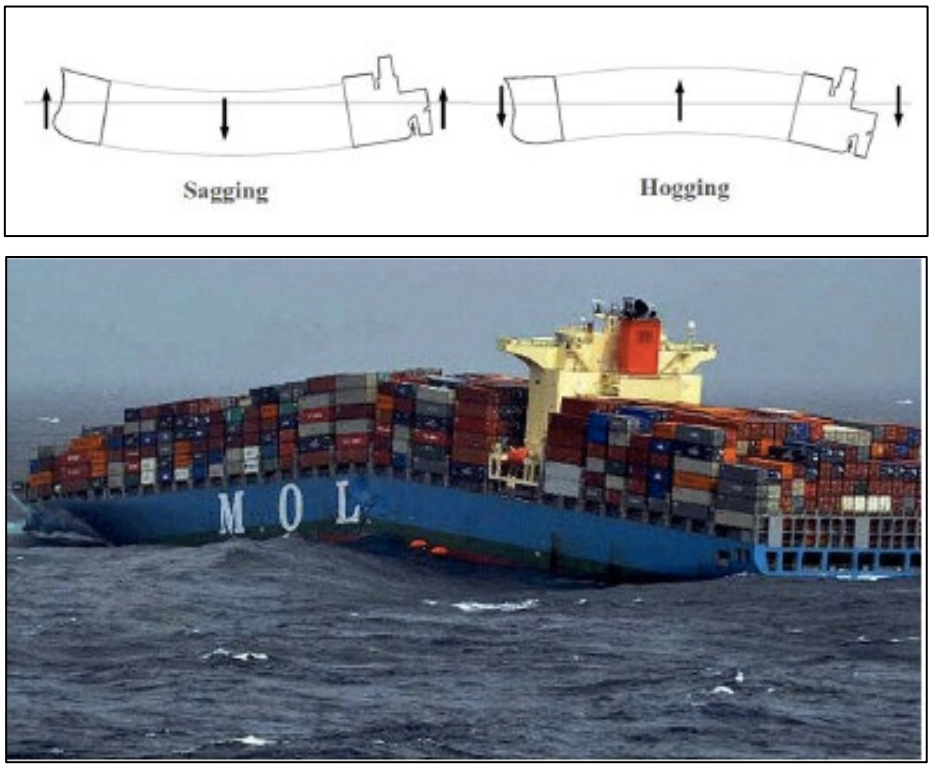


Figure 6: Sagging and Hogging of Ship Hull and Hull Failure
(Source: Constanta Maritime University)

In terms of navigation systems, penetration testers found security flaws in several ECDIS operating systems used on commercial ships.[36] Electronic Navigational Charts (ENCs) and the accompanying functionalities could be manipulated and/or deleted without the knowledge of the crew. Further, an experiment conducted by the Norwegian Defence University revealed that with a specific malware installed, attackers were able to display false positional data on the ECDIS and also trigger a non-reversible shutdown with a "blue-screen of death".[37] Ships on passage with inaccurate navigational data or a sudden loss of all ENCs or use of ECDIS may mean reduced situational awareness at sea and is exceptionally concerning as more ships adopt complete electronic-charting, diverging from even having paper charts as backup.

In another incident, cyber criminals reportedly took control of the navigation systems[38] of a German-owned container vessel en route from Cyprus to Djibouti. The systems were recovered only after bringing in IT experts.[39] These examples are once again evidence that actors have the abilities to influence a ship's OT systems and in-turn impact its interaction with the physical world.[40]

Systems Ashore

Maritime infrastructure ashore is similarly susceptible to cyber-attacks. Terminals and ports are integral parts of the maritime transport environment and are increasingly connected. Port IT infrastructure such as container tracking systems and cargo handling systems are all possible vulnerabilities which have seen their fair share of attacks.[41] Between 2011 to 2013, drug smuggling syndicates hired hackers[42] and infiltrated the Port of Antwerp's cargo tracking system. The breach allowed actors to access data such as location and security particulars of the containers, allowing them to send in a truck before the legitimate owners of the container showed up. The infiltration was reportedly through a combination of malicious software sent to staff of the port and key-logging devices which allowed remote access to the port's cargo management systems.[43]

Taken to the extreme, actors could influence commerce and disrupt important sectors such as healthcare by tampering with cargo information and delaying the delivery of important medical equipment. The theft of dangerous materials or components could also be possible and its implications potentially disastrous.[44]

Shipping and shipbuilding companies are similarly susceptible to attacks. In 2017, Maersk was hit with a complete IT system outage due to a ransomware attack. All 50,000 laptops and back-up servers were encrypted, forcing Maersk to take orders via phone calls. With 20% of the world's shipping handled by Maersk, the seriousness of this attack was evident in New Jersey where over 3,000 trucks lined up on the highway leading to port since there were no systems to handle the containers coming in and where to bring them. The estimated cost of this incident is US$350 million and it took Maersk several weeks to restart its IT network.[45]

Starting with Maersk in 2017, all four of the largest shipping companies in the world have now been hit by cyber-attacks of varying degree. Other examples include the attack on Australia-based ferry and defence shipbuilding company Austal, where perpetrators infiltrated data management systems and offered proprietary information for sale on the dark web while extorting ransom from Austal.[46] Another notable case is the Colonial Pipeline[47] cyber-attack that occurred in May this year. In a ransomware-style attack, the entire supply network was forced to shut. This pipeline was critical to several naval bases along the east coast and stayed non-operational for eight days.[48]

Aids to Navigation (AtoNs) have traditionally been physical objects like buoys and beacons. Virtual AtoNs, which are populated through the AIS infrastructure and generally controlled by maritime authorities, have been introduced although they operate unencrypted and unauthenticated. Spoofed virtual AtoN signals can mislead ships and, with malicious intent, actors could create virtual AtoNs and influence the tracks adopted by vessels and potentially lead them into danger.[49]

In Ponce De Leon Inlet, Florida, four virtual AtoNs were planted and together they indicated a safe approach although the depth of water is a mere one metre throughout (refer to Figure 7). Despite the US Coast Guard (USCG) having the sole authority in the US to transmit signals for virtual AtoNs, there are no means to authenticate the sender of these AIS signals. This curious incident remains unsolved.[50]

Issue 42, 2021

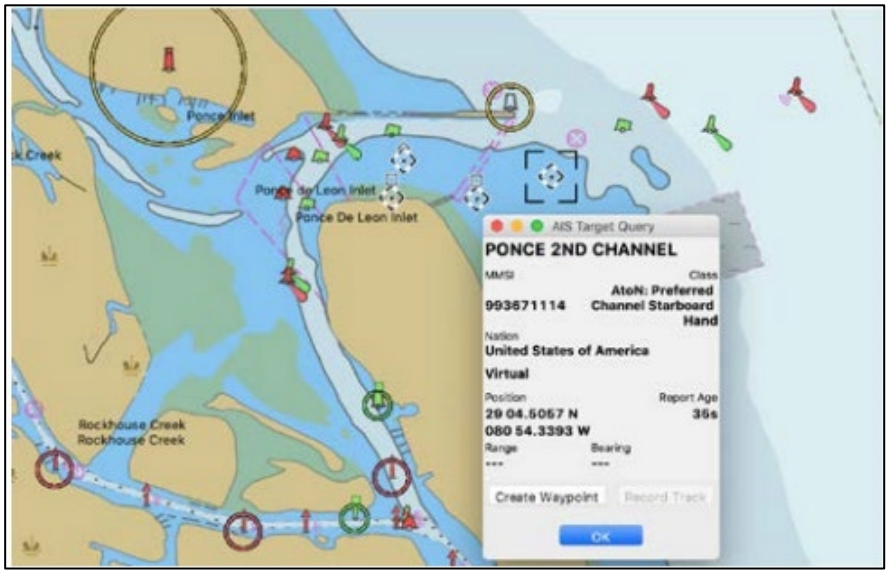


Figure 7: Virtual AtoNs Indicating a False Navigable Channel.
(Source: International Journal on Marine Navigation and Safety of Sea Transportation)

Possible Cyber-attack Scenarios along the SOMS

In the previous section, relevant cases were explored and discussed. With these cases in mind, this next section attempts to illustrate a possible scenario along the SOMS. The different categories of actors[51] and their motivation would also be an additional factor for consideration (refer to Figure 8).

Group	Motivation
Accidental actors	■ No malicious motive but still end up causing unintended harm through bad luck, lack of knowledge or lack of care, eg by inserting infected USB in onboard IT or OT systems.
Activists (including disgruntled employees)	■ revenge ■ disruption of operations ■ media attention ■ reputational damage
Criminals	■ financial gain ■ commercial espionage ■ industrial espionage
Opportunists	■ the challenge ■ reputational gain ■ financial gain
States **State sponsored organisations** **Terrorists**	■ political/idealogical gain eg (un)controlled disruption to economies and critical national infrastructure ■ espionage ■ financial gain ■ commercial espionage ■ industrial espionage ■ commercial gain

Figure 8: Actors and Their Motivation.
(Source: IMO Guidelines on Cyber-security onboard Ships)

Potentially State-backed Cyber-criminals, Hacktivists, Terrorists and Sea-robbers

The CEO of Naval Dome cited in the Singapore Maritime Technology Conference of 2019 that a ship can be used as a "very effective weapon to create chaos and destruction". A ship whose systems are under control of the cyber-criminal could result in pollution, collision, grounding, or in the deliberate misuse of a ship as an incendiary device.[52]

In the same year, the Society of Maritime Industries and the UK's Department for International Trade conducted a maritime cyber wargame during the Singapore Maritime Week 2019. The cyber-security scenario was the shutting down of a vessel's power management system caused by a dormant malware within the ship's OT systems, a scenario stated to cause an "uncomfortable situation for owner, manager, charterer and cargo owners".[53]

The scenario is realistic[54] and its impact could be devastating. Actors could target shipping companies known to transport temperature-sensitive goods such as pharmaceuticals and chemical/dangerous goods and hold ships to ransom as temperature rises/falls. Sensor and alarm systems could also be infiltrated to mask alerts[55] until right before the point-of-no-return where ship managers either agree to the ransom or agree to compensate cargo owners.

Singapore has one of the world's largest refining and petrochemical complexes. This could become a prime target for environmental hacktivists to advance their cause.[56] With the SOMS being extremely porous and distances/reaction times from critical infrastructure limited, a vessel taken over by hacktivists or any type of actor would pose significant danger to coastal communities and industries. In a more nefarious scenario ("Most Dangerous Scenario") and regardless of types of actors, the first salvo would be to target GNSS signals which could be spoofed by a briefcase-sized transmitter either onboard a nearby sampan or within one of the containers carried.[57] Possibly being led off-course and towards danger, the compromised vessel could further have its ballast tanks controlled by malware while having the ballast warning systems rendered inoperable. This would thereafter lead to the victim listing significantly and, if timed right, at the narrower and riskier sections of the SOMS (the narrowest section measures 0.5nm in the west-bound lane on the Traffic Separation Scheme along the Singapore Strait and south of Pulau Sakijang) (refer to Figure 9).

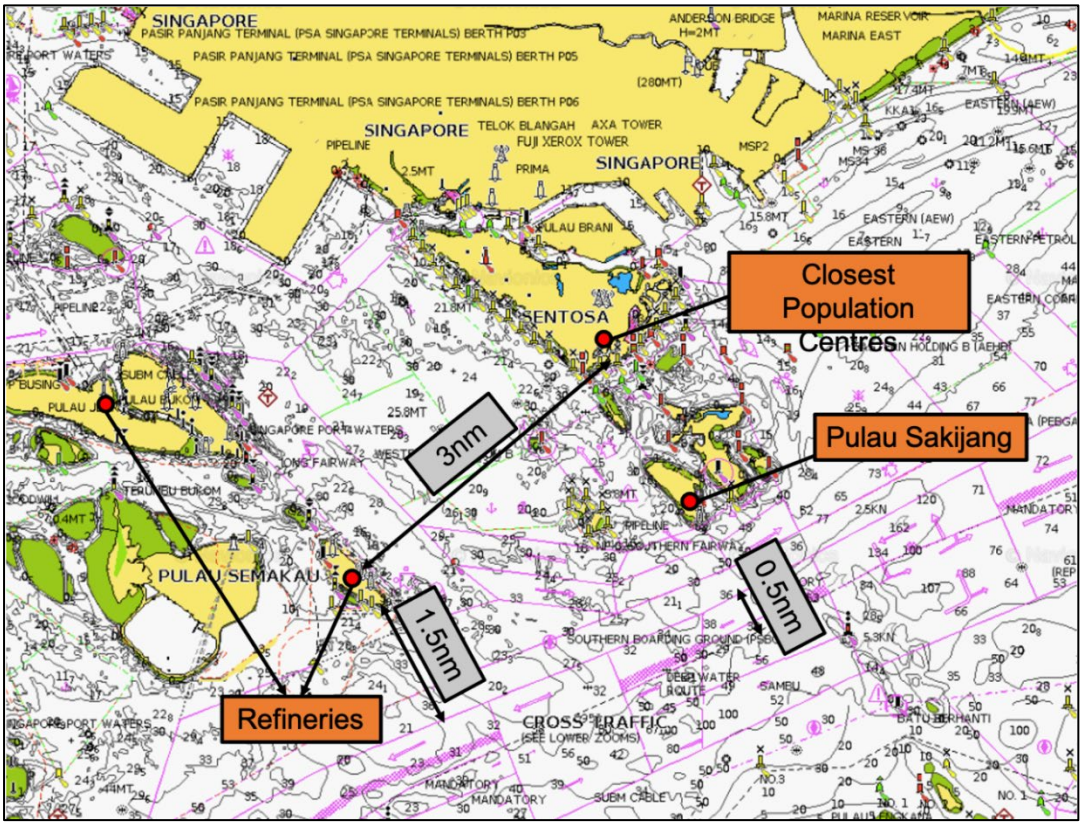
This would compel the victim to remain stationary and possibly already in close proximity to danger while waiting for mayday calls to be answered by the neighbouring port authorities. Should this step be inadequate, all ECDIS including back-up consoles could be assaulted with a "blue-screen", reducing the victim's situational awareness and anti-grounding capabilities.

With the right motivation, skillset and taking this scenario up a notch, perpetrators could have targeted vessels with masters that are pilot-exempt in the SOMS, conducted the attack during the cover of darkness, conducted GNSS spoofing to directly influence a grounding/collision situation and conducted AIS spoofing to momentarily obstruct Vessel Traffic Information Systems (VTIS) by

Issue 42, 2021

introducing thousands of ghost contacts around the vicinity of the attack/victim. MMS channels employed in the SOMS could further be jammed such that rescue operators are severely impeded when attempting to establish links with the victim.

Similar scenarios could also happen along critical entrances to the oil refinery complexes in the southern region of Singapore (An oil refinery stands 1.5nm from the west-bound Traffic Separation Scheme, which amounts to 7.5 minutes at 12 knots. An oil refinery measures 3nm from closest population centres) (refer to Figure 9). A cyber-induced collision and the time required to salvage would result in a stand-still as VLCCs bound for Singapore "wait in line" along the SOMS or are re-routed to other ports. Environmental degradation stemming from hazardous materials being discharged due to such "accidents" should also be considered. Lastly, with oil refinery complexes, the most devastating impact would be what the CEO of Naval Dome cited where ships are used as "incendiary devices" to result in chain explosions. Terrorists could adopt similar *modus operandi* to spread fear and advance their cause through violence and destruction.



Issue 42, 2021

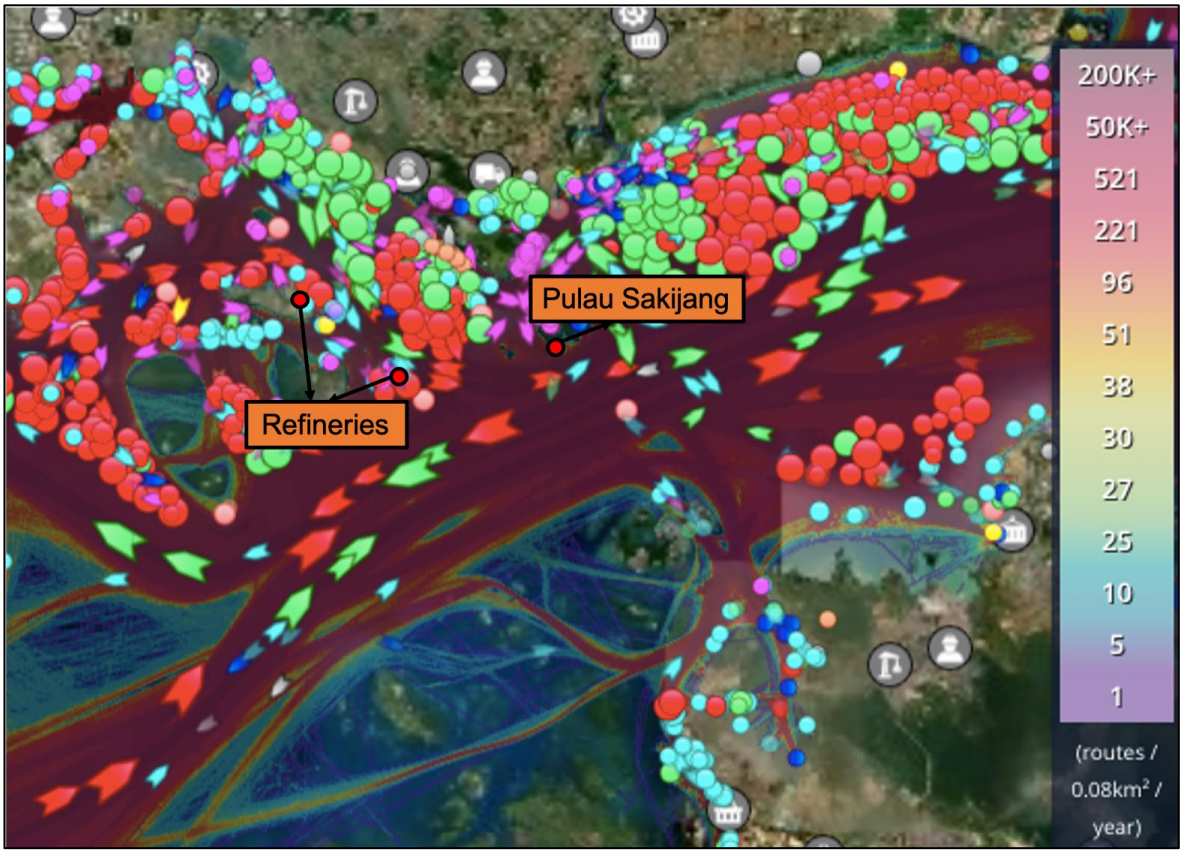


Figure 9: Key Ranges and Density of Traffic along the Singapore Strait (Source: Navionics.com & MarineTraffic.com)

Sea robbery along the SOMS reportedly increased in the first half of 2021[58] (refer to Figure 10). Although these crimes are predominantly limited to small-time actors focused on petty thefts instead of a Somali-style piracy attack,[59] they remains a threat to the maritime commons.

Issue 42, 2021

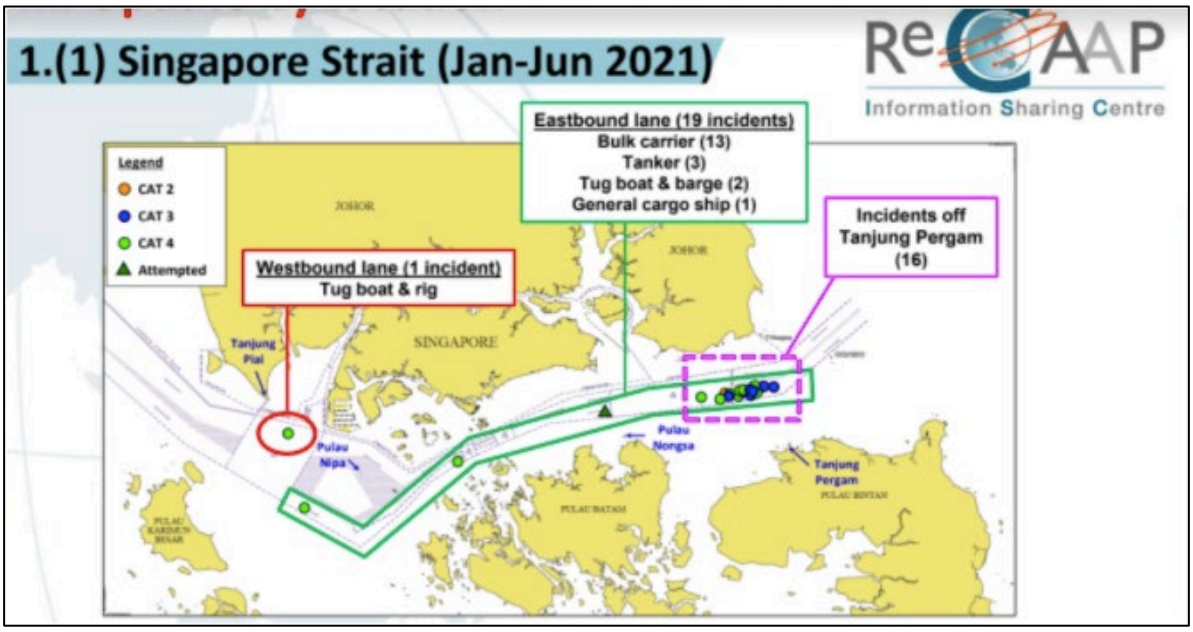


Figure 10: Cases of Sea Robberies along the Singapore Strait (Jan–June 2021)
(Source: ReCAAP Information Sharing Centre)

Increased sophistication of the criminal fraternity along the SOMS could lead to cyber-induced piracy/sea-robbery events. For instance, actors could adopt GNSS spoofing and divert targets to waters controlled by syndicates or waters known to have weaker policing. Other possibilities include targeting ships and attacking critical OT systems such as propulsion and power management systems to momentarily paralyse a victim before carrying out piracy/sea-robbery. With the rise of HaaS and GNSS-spoofing devices becoming easily accessible,[60] cyber-induced sea-robberies and piracy attacks may soon be within sight.

State-backed Actors and State Actors

State actors could also influence maritime security through the cyber domain. In May this year, Singapore unveiled an OT Cybersecurity Expert Panel and a panellist remarked that his company "tracked a state-linked hacking group which has been targeting Singapore port authorities and maritime sector".[61]

It could be expected that state-actors/state-backed actors would come to have an even greater participation in cyber-attacks on the maritime ecosystem to achieve various geopolitical and geoeconomic outcomes. These assaults have been regarded as effective grey zone vectors where plausible deniability is combined with serious real world ramifications, as seen in Russia and Ukraine.[62] (refer to Figure 11).

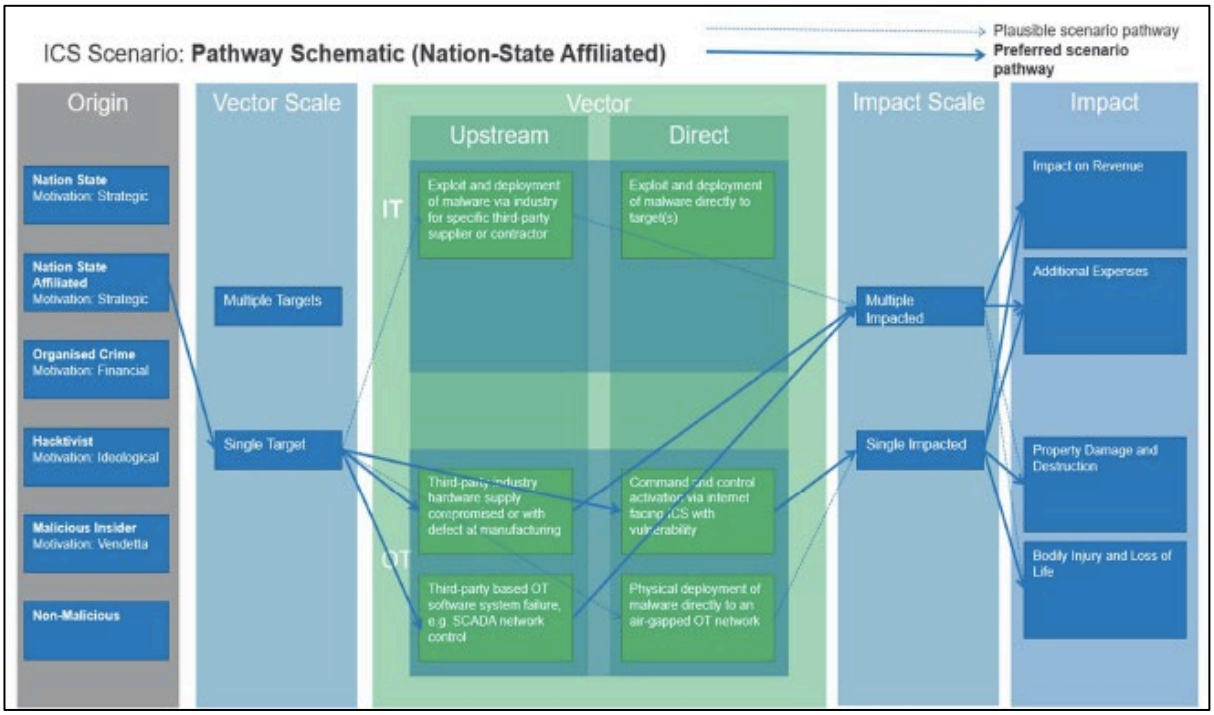


Figure 11: Possible ICS/OT Attack Pathway of a State-backed Actor
(Source: Lloyd's List and CyberCube's Research on Threats to Maritime OT Systems)

The same study by Lloyd's List asserted that the successful breaching of critical OT systems such as a ship's ballast or navigational systems is no walk in the park and would require a well-planned reconnaissance phase where "beacons" create network blueprints of the target. The creation of the actual payload which conducts the "attack" on the OT systems is bespoke and based on the network blueprint.

No doubt with the rise of HaaS[63] and in-turn the accessibility of this technology to independent actors, state-backed or state actors are more likely to have the resources, capabilities, time and strategic motivation to have a persistent attack vector towards the targeted aspect of the maritime ecosystem.[64] [65]

Geopolitical outcomes that states could desire include influencing a target's foreign policy. This could be conducted through non-attributable cyber-attacks such as assaulting the target's shipping sector surrounding a particular type of goods or similar scenarios highlighted in the previous section where commercial vessels are targeted.[66] Other possibilities include sabotaging the target's maritime resources and coastal population by inducing an episode of environmental pollution by conducting cyber-attacks on tankers.

Maritime territorial disputes or delimitation of maritime boundaries could also involve cyber-attacks where commercial ships like fishing trawlers spoof their AIS identity to conduct illegal fishing or create ghost ships to initiate illegal fishing on opponents by fabricating facts on the ground. Similar cases were cited in the previous section including the case of *Stena Impero* and the recent case between the Royal Navy (RN) and Russia where AIS positions of RN ships were spoofed and shown to be in the vicinity of Crimea.

Taken together, these scenarios could occur along the SOMS or in the neighbouring South China Sea. State-backed or state actors are more likely to have the strategic objective, resources, time and motivation and are thus an important threat vector to consider.

Impact of Maritime Cyber-attacks

The University of Cambridge Centre for Risk Studies offered a scenario of an infected cargo-management software which corrupts the fleet's cargo manifest. The malware thereafter gets transferred to port management systems and impacts other ships. Adopting this scenario, a Singapore-based public–private initiative that assesses cyber risks estimates losses of over US$110 billion and the crippling of supply chains across the world as ports and ships get thrown into confusion.

Asia will experience most of the impact of this fallout with US$27 billion in indirect economic losses expected.[67]

These numbers do not seem surprising given that the MV *Ever Given* and her saga in the Suez Canal this year was estimated to cost global trade between US$6–10 billion a week and reducing annual trade growth by 0.2 to 0.4 percentage points.[68]

A study by Allianz Global on cyber-induced collision in an "environmentally-sensitive" location showed losses would amount to US$4 billion when taking into account disruptions, salvage operations and loss of property. Attacks on port infrastructure such as ransomware attacks on the Ports of Barcelona and San Diego in 2018 similarly chalked up significant losses.[69] Apart from the more apparent economic repercussions, bodily injuries/deaths, damage to infrastructure, environmental pollution, loss of confidence, fear, and reputational risk can all be associated with maritime cyber-attacks.[70]

Along the SOMS, Port Klang, Port of Tanjung Pelepas and Port of Singapore are the three busiest ports in Southeast Asia. The shipping sector in Singapore accounts for 7% of her GDP[71] while Malaysia's maritime sector which consists of oil and gas, fisheries and maritime-related industries accounts for 40% of her GDP.[72] Therefore a significant cyber-induced attack along the SOMS would have direct implications and repercussions to reputation and confidence that took countries along the SOMS decades to build.

Maritime Cyber-security Game Plan in the Region

Internationally, the IMO adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems in 2017. Essentially, IMO is encouraging shipping companies to take into account cyber risk management according to the guidelines promulgated by the IMO and include the steps/initiatives taken by companies in ships' overall Safety Management Systems.

This is to be completed prior to the first annual verification of the company's Document of Compliance after 1 January 2021.[73] Authorities in Singapore and Malaysia issued a shipping circular to remind relevant stakeholders of the IMO resolution and the deadlines.[74]

Along the SOMS, Singapore first mooted a cyber-security masterplan to protect OT systems from cyber-attacks in 2019. The masterplan covers critical sectors such as water supply and transport, and aims to bolster defence against attacks by improving information exchange between public and private sectors. An OT Cyber-security Information Sharing and Analysis Centre, and an OT Cyber-security Expert Panel were also set up as part of the masterplan.[75] At the sectoral level, the Maritime Port Authority of Singapore opened the Maritime Cybersecurity Operations Centre in 2019. The 24/7 centre monitors maritime CIIs and has capabilities to respond against cyber-attacks.[76]

Malaysia's National Cyber Security Agency was established in 2017 and reports to the National Security Council while the Cyber Security Strategy 2020–2024 was introduced in 2020 to stipulate frameworks for specific domains, although maritime related cyber concerns were not specified.[77] Malaysia's Ministry of Transport which oversees port authorities and the shipping sector has also been working with the American Bureau of Shipping (ABS) Advanced Solutions as their cyber-security partner.[78]

In Indonesia, President Joko Widodo strengthened Indonesia's National Cyber and Crypto Agency (BSSN) in April this year by having it directly under the auspices of the president instead of ministries and other governmental bodies. This move is expected to improve BSSN's agility and authority. Indonesia is also working on the nation's first national cyber-security strategy, frameworks on the management of a national cyber crisis, and greater cooperation with the Australian Government in handling cyber-security in the region.[79] It appears that Indonesia does not currently have a dedicated maritime cyber-security game plan.

Regional groupings also saw the rising importance of cyber-security. The ASEAN Defence Ministers Meeting (ADMM) this year formalised an ADMM Cyber-security and Information Centre of Excellence based in Singapore.[80] An ASEAN–Japan Cyber-security Capacity Building Centre was also launched in 2019 to promote intra-regional collaboration on the rising threat.[81] Other ongoing initiatives include a concept paper on the ASEAN Cyber Defence Network which aims to link cyber-defence operation centres of member states for a concerted effort against cyber-threats from actors including extra-regional ones.[82]

Challenges in Improving Maritime Cyber-security

Despite emphasis on the international and governmental fronts, there remain multiple challenges and vulnerabilities to be addressed by both maritime practitioners and the international community.

The challenge of addressing maritime cyber-security for systems in the general environment such as civilian GNSS and AIS lies with the scale of the issue. It requires an international effort and involves an array of stakeholders. Although there are individual countries attempting to resolve the lack of security for GNSS and AIS, there has been limited impetus for change.[83]

On OT systems, overhauling and hardening OT systems on ships mean additional costs and time away from generating revenue. This challenge is aggravated by the absolute need of OT systems to run uninterrupted in most cases. OT systems also have long lifecycles, exist in a complex "system of systems" and are often not designed with security capabilities due to lack of computing resources.[84] *They are also generally more complex than traditional IT systems since multiple disparate OT systems interface and interact with each other and hence retrofitting this OT software is no trivial task.*[85]

In addition to hardening systems onboard, a survey conducted by BIMCO revealed that more than half of respondents believe "poorly trained staff coupled with a lack of cyber-security protocols within a shipping company" are causes of financial and operational woes to container lines.[86]

Crew onboard were cited to be increasingly targeted by cyber-criminals to infiltrate the network through methods such as emails and website links, compromised storage devices and other spear-phishing and social engineering attempts. Incentives to cover up deliberate disruptions of OT systems, to avoid revealing vulnerabilities and impacting reputation, further exacerbate the challenge for the community.[87]

Systems ashore face a similar challenge of poor cyber-awareness amongst personnel. Susceptibility of cyber-attacks is also heightened due to trends such as HaaS and the perceived deep pockets of shipping companies and port authorities.[88] Shore systems, similar to OT systems onboard ship, are also open to a more insidious and difficult to detect supply chain-type attack where adversaries insert dormant vulnerabilities to intermediate software and/or hardware to be manipulated in future. In 2020, a relevant case was observed in the US where officials seized a foreign-built transformer due to the discovery of electronics "that should not have been part of the transformer". These electronics were reportedly capable of enabling remote control of the transformer and sending bogus readings of parameters, and in-turn sabotaging parts of the US power grid.[89] The increased homogeneity of sub-systems adopted in OT is likely to further increase risks of widespread compromise, infiltration and attacks.[90]

Lastly, as the risk–reward ratio and accessibility to technology improve for cyber-criminals, more "ransomware gangs" are expected to surface and to continuously improve their TTPs around cyber-security. Further, with state-backed "Privateers" joining the fray, attacks on systems ashore become a question of when, rather than if.[91]

Issue 42, 2021

SECTION III

Evaluation

The IMO's resolution on Maritime Cyber Risk Management is a step forward although policing the resolution is dependent on port authorities around the world and it remains to be seen if these measures produce results in reducing cyber-attacks within the maritime community.

Countries along the SOMS have displayed some degree of readiness on the national and sectoral levels to examine and counter the risks of maritime cyber-attacks. Through national, regional and intra-regional cooperation and cyber-security working groups, benefits such as information exchange, intelligence and early-warning could be realised.

Ships and shipping companies form a large bulk of this ecosystem. The 2020 Safety at Sea and BIMCO Maritime Cyber Security Survey had 77% of respondents indicating that they are at a medium to high risk of cyber-attacks. Despite this, close to two-thirds of respondents stated that they were not currently employing solutions to protect ship OT systems. Some respondents described their company policy on OT cyber-risks as "careless".[92] In other words, there are a significant number of ships plying the ocean this very moment without additional cyber-security protections on their operational infrastructure. It is therefore paramount that countries along the SOMS look beyond working groups and work on regulatory changes to hasten the adoption of maritime cyber-security solutions.

Recommendations

Mitigating Vulnerabilities of Systems in the General Environment

The danger of GNSS spoofing and jamming could be mitigated by adopting smart receivers[93] capable of receiving signals from multiple GNSS constellations including GLONASS, Galileo and BeiDou. Such capabilities increase the difficulty for actors since the additional positioning information allows for anomaly detection.

Other alternative strategies, such as the eLoran[94] system and Galileo's paid Commercial Authentication Service (CAS) where signals are encrypted, are in development and would reduce the occurrences of GNSS spoofing and jamming.[95] Countries are also working on free-to-use encrypted GNSS services such as Galileo's OSNMA and GPS's Chimera which several brands of "future-proof multi-frequency GNSS receivers" have been marketed to be compatible with.[96]

The US Navy is further developing an Automated Celestial Navigation System which takes away the need for manual sextant measurement of celestial bodies, a positioning method that reduces reliance on satellite-based positioning systems. Companies in the project are also working on using satellites on Low-earth Orbit (LEO) for calculation of positional data to improve availability. This is expected to be aided by Elon Musk's Starlink project which aims to launch more than 700 LEO satellites in the next few years, allowing ships to "always have one handy to take a reading".[97]

As these developments become widespread and commercially available, ships would have more options to safeguard against GNSS spoofing attacks. However, unless mandated, the speed of adoption is likely to be commensurate with the perceived threat of an attack. AIS could similarly be improved by encrypting AIS signals. One possibility cited by Kessler is a protected AIS (pAIS) software which uses a public-key cryptography method to provide authentication of the sender and guarantee the integrity of the message.[98] The maritime community will need to agree on application-layer design guidelines and technical details including the setup of a dedicated Public Key Infrastructure.[99] The implementation of anomaly detection techniques by VTIS to detect and flag suspicious AIS activities could further reduce the threat of AIS spoofing to maritime authorities monitoring vessel traffic.[100]

Mitigating Vulnerabilities of Systems onboard Ships and Systems Ashore

Cyber-security companies dedicated to securing maritime OT systems, designing new OT systems with cyber-security needs such as computing power and compatibility with security patches (pressured by end-users such as ship owners), and the adoption of "defence in depth"[101] should all be considered.[102]

Other established frameworks that organisations could reference include Lockheed Martin's Cyber Kill Chain methodology for network defence. This framework emphasises that the defender has the advantage since actors must be successful in all seven stages of exploits whereas the defender simply needs one mitigation to "break the chain" and foil the attack.[103]

Several organisations including BIMCO, Cruise Lines International Association and International Chamber of Shipping (ICS) also published technical guidelines for cyber-security onboard which should be referenced by ship operators. Although IMO's technical guidelines are generic,[104] the emphasis on a "culture of cyber-risk awareness",[105] which has been echoed by many,[106] cannot be ignored and should be top-of-mind for all vessel operators and port personnel in their protection against future cyber-attacks. Port authorities along the SOMS may further consider instituting selected clauses within the technical guidelines published by BIMCO and the ICS, for ships flagged in the respective countries.[107] IMO is similarly recommended to reinforce its cyber-security guidelines and mandate selected clauses following industry consultations. These may include mandating the air-gapping of certain critical ship-board systems and the compulsory adoption of intrusion monitoring systems, establishing a foundational level of protection across the sector. An implication to consider when regulating is the resources required for enforcement.

Role of MLEAs, Port Authorities and Regional Groupings

With the increase in cyber-risks, authorities along the SOMS need to have full cognisance of what an attack might look like and the potential impact of these incursions, while preparing, drilling and communicating pre-planned responses for both commercial ships and first-responders such as the coast guard or the navy. Scenarios of maritime cyber-attacks should be included in tactical guides and operations plans of the individual Maritime Law Enforcement Agencies (MLEAs) on top of the current operations plans against traditional maritime security threats they are faced with.

MLEAs along the SOMS may consider a set of procedures and agencies to establish two-way links such as with the aforementioned 24/7 Maritime Cyber-security Operations Centre and the Information Fusion Centre (IFC).[108] Responses need to be coordinated, joint and agreed upon by countries along the SOMS and could involve ongoing joint patrols such as the Malacca Strait Sea Patrol (MSSP) which brings together Thailand, Malaysia, Singapore and Indonesia. Within these centres, organic cyber capabilities and technical expertise will likely require sustained emphasis and investment.

The human factor in our resistance against cyber-attacks should also be worked on. Port and maritime authorities could introduce a joint maritime cyber-security literacy programme where real-world cases are discussed and cyber-security pitfalls highlighted. These could be regulated and mandated for maritime practitioners such as crew onboard ships flagged in the region and personnel employed in the maritime public sector. This could be tiered according to areas of responsibilities and could be carried out through micro-credentialled programmes by universities or polytechnics.[109]

Cyber-security in other commercial infrastructure such as energy, telecommunications and the financial systems are much more developed.[110] There are opportunities for the maritime sector to build on cyber-security lessons gleaned from these sectors such as the US financial sector's regular and realistic joint exercises which build confidence and collaborative links between stakeholders and governmental entities. Energy sectors on the other hand have normalised 24/7 cyber-security operation centres monitoring for malicious system behaviours across the power grid.[111]

Maritime authorities may consider incorporating these defensive efforts with present infrastructure and frameworks. Authorities could further expand on the mandate of forums such as ADMM Cyber-security and Information Centre of Excellence and replicate conferences similar to the NATO International Conference on Cyber Conflict (CyCon) which gives members the platform to engage in regular red–blue team exercises. "Bug Bounty"[112] programmes partnering the private sector could also be instituted by these organisations to improve the identification and rectification loop for vulnerabilities, especially onboard ship OT systems and port IT/OT systems.

Other established information-sharing infrastructure to potentially model after includes the Regional Cooperation Agreement on Combating Piracy and Armed Robbery (ReCAAP).[113] For these forums to be fruitful, authorities may have to mandate the reporting of cyber-attacks and improve the transparency of these occurrences since there are clear incentives for companies/ships to act otherwise.[114]

Potential Recourse against Perpetrators

With no clear rules of engagement when dealing with cyber-attackers, proportionate and appropriate response could be up for debate. Further, attribution remains challenging given attacker infrastructure like IP addresses and domains are almost always spoofed. Attackers' tactics, techniques and procedures, which in the past acted as fingerprints of each distinct hacker group, are also becoming harder to identify given greater use of "off-the-shelf" malware and HaaS.[115] However, when cyber-attackers are identified, control measures can be imposed. In July 2020, the European Union imposed its first ever sanction for cyber-attacks on identified individuals and entities found responsible for WannaCry and NotPetya. Sanctions imposed included a travel ban and asset freeze.[116]

Where perpetrators are identified as state-actors or clearly state-backed actors, then recourse becomes trickier. In response to the SolarWinds[117] attack, US placed sanctions and expelled 10 Russian diplomats, stopping short of further responses.[86]

A lesser-known domain that has been explored in the US is the concept of "hack-backs" where organisations publicise their employment of hackers who would engage in a counter-attack against actors should they be attacked. This offers a degree of deterrence although it remains underdeveloped and illegal in some territories.[118]

Further Research

Works by scholars, specialists and experts in the field would further improve understanding of the cyber challenges maritime practitioners face today. An overall lift in cyber-security understanding and skillsets would reduce our propensity to be the "weak links" while enabling maritime practitioners to be the first line of defence against cyber-attacks.

The previously cited 2020 Maritime Cyber Security survey conducted by BIMCO revealed that only 22% of respondents received high-quality maritime cyber-security training,[119] suggesting that more attention is required on improving cyber-security training and pedagogy. Further, the European Cyber Security Organisation (ECSO) estimates that the maritime industry has a shortfall of 50,000 to 100,000 personnel trained in cyber-security,[120] suggesting that further research into the human resource and training/development aspects of maritime cyber-security may yield long-term dividends. More studies, independent audits and research should also be conducted on key stakeholders along the SOMS. For instance, exploring maritime cyber-security readiness of ships flagged in the region through red–blue team cyber wargames, empirical research into the benefits of implementing IMO's resolution on Maritime Cyber Risk Management and scoring port cyber-security infrastructure similar to what was conducted in the US by the USCG.[121] Uncovering these weaknesses would be another step towards better management of cyber-risks along the SOMS.

Finally, vulnerabilities in the maritime ecosystem and the ongoing cyber threats and risks are expected to remain. The possible impact of failure as highlighted in this paper is dire and future plans such as the Maritime Autonomous Surface Ships (MASS) programme[122] heighten the importance of maritime cyber-security. This field should therefore continue to receive sustained study, emphasis and interest across maritime stakeholders.

Endnotes

[1] IHS Markit. "Safety at Sea and BIMCO Cyber Security White Paper" in *Safety at Sea* (2020), p. 15.
[2] Mission Secure Inc., a leading cyber-security firm, estimates that only 5–10% of the world's 90,000 commercial vessels are prepared to defend against cyber-attacks.
[3] World Economic Forum. "Consequences of Digital Fragmentation" in *The Global Risks Report* (2020), p. 63.
[4] Arampatzis, A. "The Biggest Challenges and Best Practices to Mitigate Risks in Maritime Cybersecurity" in *The State of Security* (2020).
UT News. "UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea" in *UT News Science and Technology* (2013).
[5] The OT systems in this particular study refer to the OT systems ashore such as the traffic control and vessel berthing systems, and cargo handling systems at ports. OT and IT are different in the attack outcome. An attack on IT could lead to data theft while an attack on OT could lead to injury, loss of life, asset damage or environmental impact.
[6] Androjna, A., Brcko, T., Pavic, I. & Greidanus, H. "Assessing Cyber Challenges of Maritime Navigation", *Journal of Marine Science and Engineering* (2020), p. 1.
[7] Lendvay, R. "Shadows of Stuxnet: Recommendations for US Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack", *Naval Postgraduate School Journal* (2016), pp. 5-6.
[8] Lagouvardou, S. "Maritime Cyber Security: Concepts, Problems and Models" (2018), p. 30.
[9] Delagrange, O. "Assessing the Cyber Risks of Maritime Navigation" in *Kennedyslaw* (2017), p. 3.
[10] National Strategy for Maritime Security. *National Maritime Cybersecurity Plan* (2020), pp. 3, 9-10.
[11] The Energy Information Administration (EIA) of the US Department of Energy named the SOMS as one of the world's primary crude-oil transit chokepoints. 90% of crude oil volume flowing through the South China Sea transits the SOMS and more than 100,000 vessels transit the SOMS each year, accounting for close to a quarter of the world's traded goods. Any blockade or impediment, with nefarious intent or otherwise, is expected to impact the supply of energy and raw materials to the region and beyond. With traffic expected to double over the next decade and the SOMS being one of the world's narrowest straits (at 0.5 nautical miles at its narrowest section), the difficulty of maintaining maritime safety and security along the SOMS is expected to increase.
[12] Bueger, C. "What is Maritime Security?" in *Marine Policy* (2014), pp. 4-5.
[13] Hill, J. R. "Maritime Strategy for Medium Powers" (1986), pp. 101-104.
[14] International Telecommunication Union. "Overview Cybersecurity" (2008).
[15] Fruhllnger, J. "What is a Cyber Attack? Recent Examples Show Disturbing Trends" in *CSO Australia* (2020).
[16] Morgan, C. "Cyber Attacks: The Challenge of Attribution and Response" in *Digitalshadows* (2021).
[17] Fitton, O., Prince, D., Germond, B. "The Future of Maritime Cyber Security" in *Lancaster University* (2015), p. 8.
[18] Gillespie, C. "Cyber Risks: Insurance Cover and Cyber Preparedness" in *Safety4Sea* (2018).
[19] Raine, J. "War or Peace? Understanding the Grey Zone" in *International Institute of Strategic Studies* (2019).
Sutton, H. I. "Positions of Two NATO Ships were Falsified Near Russian Black Sea Base", *United States Naval Institute News* (2021).
[21] Androjna, A., Brcko, T., Pavic, I. & Greidanus, H. "Assessing Cyber Challenges of Maritime Navigation", *Journal of Marine Science and Engineering* (2020), pp. 8-9.
[22] Above Us Only Stars. "Exposing GPS Spoofing in Russia and Syria" in *C4ADS* (2019), pp. 2-5.
[23] Using commercial off-the-shelf equipment, researchers at the University of Texas spoofed unencrypted civilian GPS signals which resulted in inaccurate positioning data. This led to an erroneous course correction executed by the vessel's crew which in-turn put the 65-metre yacht off-course.
[24] The detention of the *Stena Impero* was widely seen as retaliation to an earlier impounding of an Iranian VLCC.
[25] Bockmann, M. "Seized UK Tanker Likely Spoofed by Iran" in *Lloyd's List Maritime Intelligence* (2019).
[26] Androjna, A., Perkoviˇc, M., Pavic, I. & Miškovi´c, J. "AIS Data Vulnerability Indicated by a Spoofing Case-Study" in *Applied Sciences* (2021), pp. 2-6.
[27] Zwirko, C. "NK Vessels Exploiting Tracking System Flaws to Evade Sanctions", *NK News* (2019).
[28] Israeli cyber-security company with focus on maritime cyber-security.

[29] Ovcina, J. "Naval Dome: 400% Increase in Attempted Hacks Since Feb 2020" (2020).
[30] Lloyd's, CyberCube. "Cyber Risk: The Emerging Cyber Threat to Industrial Control Systems" (2021), pp. 12-14.
[31] Cyber risk analytics company previously owned by leading cyber-security company Symantec.
[32] Lloyd's, CyberCube. "Cyber Risk: The Emerging Cyber Threat to Industrial Control Systems" (2021), pp. 16-17.
[33] Robin, P., Baezner, M. "Hotspot Analysis: Stuxnet" in *Center for Security Studies Zurich* (2017), pp. 7-9.
[34] In 2001, an Australian man was charged with hacking into a computerised waste management system in Queensland, causing millions of litres of raw sewage to spill into local parks, rivers and grounds of a hotel.
[35] Zagan, R. & Raicu, G. "Understanding Cyber Risk onboard Ship and Ship Stability" in *The Annals of Dunarea de Jos* (2019), pp. 6-10.
[36] Lagouvardou, S. "Maritime Cyber Security: Concepts, Problems and Models" (2018), pp. 68, 88.
[37] Hareide, O., Josok, O., Lund, M., Ostnes, R. & Helkala, K. "Enhancing Navigator Competence by Demonstrating Maritime Cyber Security", *The Journal of Navigation – Royal Institute of Navigation* (2018), pp. 5-11.
[38] Similar to most overt reports of cyber-attacks, information is limited in this particular case.
[39] IHS Markit. "Hackers Took Control of Container Ship's Navigation Systems for 10 Hours" in *IHS Fairplay* (2017).
[40] Other relevant examples in the maritime realm include attacks on oil rigs. Although details of this case remain elusive, several research papers have cited the 2014 incident off the coast of Africa where a malicious cyber-attack caused an oil rig to list to one side and shut production for a week. Mike Ahmadi, global director at Synopsys, stated that vulnerabilities of control systems responsible for managing pontoons that keep offshore rigs afloat could be targeted and controlled to influence the stability of the rig.
[41] Marsh. "The Risk of Cyber-attack to the Maritime Sector" in *Global Marine Practice* (2014).
[42] Hackers-as-a-Service or HaaS creates a low-barrier of entry for malicious actors since technical skillsets which are challenging to acquire are now available for sale.
[43] Bateman, T. "Police Warning after Drug Traffickers' Cyber-attack", BBC (2013).
[44] Tam, K., Papadaki, M., & Jones, K. "Threats and Impacts in Maritime Cyber Security" in *Engineering & Technology Reference* (2016) pp. 3-4.
[45] Cimpanu, C. "All Four of the World's Largest Shipping Companies Have Now Been Hit by Cyber-attacks" in *zdnet* (2020).
[46] Hannemann, W. "Key Takeaways from 3 Recent Cyber Attacks in Shipping" in *Dualog* (2019).
[47] Colonial Pipeline is one of the largest refined fuel pipelines in the US.
[48] Reeder, J. "Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack" in *GTLAW* (2021), pp. 15-17.
[49] Androjna, A., Perkovi˘c, M., Pavic, I. & Miškovi´c, J. "AIS Data Vulnerability Indicated by a Spoofing Case-Study" in *Applied Sciences* (2021), pp. 7-8.
[50] Kessler, G. "Protected AIS: Demonstration of Capability Scheme to Provide Authentication and Message Integrity", *International Journal on Marine Navigation and Safety of Sea Transportation* (2020), p. 281.
[51] According to Lockheed Martin, the modern-day attackers are more sophisticated, well-resourced, trained and adept at launching skilfully planned intrusion campaigns called Advanced Persistent Threats (APT).
[52] World Maritime News. "Naval Dome: Shipping Needs to Be on Red Alert for Cyber Attack" (2019).
[53] Hellenicshippingnews. "Virus-hit Boxship Takes Centre Stage at Singapore Cyber Wargame", *International Shipping News* (2019).
[54] As discussed in prior sections, malware inserted into IT and OT systems onboard ships may lie dormant until a pre-coded set of conditions are met before launching an assault. These conditions may include coordinates, time or a set of actions.
[55] Masking of sensor outputs was seen in the Stuxnet attack.
[56] Environmental hacktivism was first observed a decade ago conducted by hacker group Anonymous who launched a campaign of cyber-attacks in support of green causes. Companies like Monsanto were targeted and big oil corporations like Exxon Mobil were reportedly in the crosshairs of the organisation.[43] This suggests the possibilities of environmental hacktivism cannot be discounted and should occupy the minds of policymakers and maritime practitioners.
[57] Tam, K., Papadaki, M., & Jones, K. "Threats and Impacts in Maritime Cyber Security" in *Engineering & Technology Reference* (2016). pp. 3-4.

[58] Hand, M. "Piracy and Armed Robbery Incidents Increase in Singapore Strait", *Seatrade Maritime News* (2021).
[59] These attacks are predominantly CAT 3 incidents and they are defined by ReCAAP as attacks by 1–6 men, sometimes armed with weapons like machetes, and ship crew are generally unharmed. Where losses are reported, stores and engine spares were the commonly targeted items.
[60] A Chinese cyber-security company demonstrated at a hacking convention in Las Vegas that a GNSS-spoofing device can be easily procured and would cost a mere US$300.
[61] Chee, K. "Cyber Threats to Critical Infrastructure Systems Still Low in Singapore but Maritime Sector a Target", *The Straits Times* (2021).
[62] Kremidas-Courtney, C. "Countering Hybrid Threats in the Maritime Environment" in *Centre for International Maritime Security* (2018).
Zetter, K. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", *Wired* (2016).
[63] Yaffa, J. "How Hacking Became a Professional Service in Russia", *The New Yorker* (2021).
[64] Lloyd's, CyberCube. "Cyber Risk: The Emerging Cyber Threat to Industrial Control Systems" (2021), pp. 27-28.
Lendvay, R. "Shadows of Stuxnet: Recommendations for US Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack", *Naval Postgraduate School Journal* (2016), pp. 57-58.
[65] The Stuxnet malware was developed only after one year of reconnaissance involving a "beacon" which maps the network blueprint and operating parameters of systems connected. The level of detail required for the Stuxnet attack was to the exact RPM adopted by the centrifuges which were controlled by the OT systems and details of the sensors and monitoring systems.
[66] US Department of Homeland Security. "Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar" in *US DHS* (2019), pp. 13-14.
[67] Bielby, K. "A Maritime Cyber Attack Could Cost $110 Billion and Cripple Global Supply Chains" in *Homeland Security US* (2019).
[68] Russon, M. "The Cost of the Suez Canal Blockage", BBC (2021).
[69] Allianz Global. "Safety and Shipping Review 2019" in *Allianz* (2019), pp. 38-29.
[70] Tam, K., Papadaki, M., & Jones, K. "Threats and Impacts in Maritime Cyber Security" in *Engineering & Technology Reference* (2016). pp. 5-6.
[71] Enterprise Singapore. "Industry Profile" in *Enterprises* (2020).
[72] Hamzah, B. A. "Maritime Sector in need of Reform", *New Straits Times* (2019).
[73] International Maritime Organization. "Maritime Cyber Risk" in *IMO* (2017).
[74] Goh, C. H. "Maritime and Port Authority of Singapore Shipping Circular No.15 of 2020" in *MPA* (2020), pp. 1-2.
Jabatan Laut Malaysia. "Maritime Cyber Risk Management" in *Marine Department Malaysia* (2018), pp. 1-2.
[75] Baharudin, H. "New Cyber-security Masterplan Launched to Protect Critical Sectors", *The Straits Times* (2019).
Chee, K. "Cyber Threats to Critical Infrastructure Systems Still Low in Singapore but Maritime Sector a Target", *The Straits Times* (2021).
[76] MPA. "New 24/7 Maritime Cybersecurity Operations Centre to Boost Cyber Defence Readiness" in *Maritime Port Authority of Singapore* (2019).
[77] National Cyber Security Agency Malaysia. "Cyber Security Strategy 2020–2024", in *National Security Council* (2020).
[78] Tan, J. & Zulfa, M. "Maritime Cybersecurity in Malaysia" in *Malaysia Institute of Maritime Affairs* (2021), pp. 5-7.
[79] Keller-Nabbs, G., Wibawanto, R.M., & Widodo, N. "Indonesia Responds to the Cyber Dark Side", Lowy Institute (2021).
[80] The centre is designed to facilitate cooperation on cyber-security and information sharing within the defence sector and amongst ASEAN members.
[81] Parameswaran, P. "ASEAN Cyber Challenge in the Spotlight with New Center", *The Diplomat* (2021).
[82] Gady. F. "China Spies on India and ASEAN Member States", *The Diplomat* (2015).
[83] Caprolu, M., Pietro, R. D., Raponi, S., Sciancelepore, S., & Tedeschi, P. "Vessels Cybersecurity: Issues, Challenges, and the Road Ahead" in *Qatar National Research Centre* (2020), pp. 2-3, 6.
[84] Arampatzis, A. "The Biggest Challenges and Best Practices to Mitigate Risks in Maritime Cybersecurity" in *The State of Security* (2020).
[85] Arampatzis, A. "The Biggest Challenges and Best Practices to Mitigate Risks in Maritime Cybersecurity" in *The State of Security* (2020).

[86] Tan, J. & Zulfa, M. "Maritime Cybersecurity in Malaysia" in *Malaysia Institute of Maritime Affairs* (2021), p. 8.
[87] Androjna, A., Brcko, T., Pavic, I. & Greidanus, H. "Assessing Cyber Challenges of Maritime Navigation", *Journal of Marine Science and Engineering* (2020), p. 1.
[88] Sadek, N. "Shipping Companies Confront Cyber Crooks as Economies Reopen" in *Bloomberg Government* (2021).
[89] Middendorf, J. W. "Could China Hack Our Electric Grid?" in *The Heritage Foundation – Cyber Security* (2021).
[90] Yaacoub, J. A., Salma, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. "Cyber-physical Systems Security: Limitations, Issues and Future Trends" in *Microprocessors and Microsystems* (2020), pp. 7-8.
[91] Zappone, C. "Pirates of the Cyber Seas: How Ransomware Gangs Have Become Security's Biggest Threat", *The Sydney Morning Herald* (2021).
[92] Mission Secure. "A Comprehensive Guide to Maritime Cybersecurity" (2020), p. 4.
[93] Multi-frequency receivers are designed to tap into all available satellite constellations to deliver more accurate, reliable and robust positioning data.
[94] The Enhanced Long-range Navigation (eLoran) system uses terrestrial radio broadcasts for positioning, providing very accurate positioning data and is seen to be making a return as a backup to GNSS. Spoofing and jamming risks are reduced significantly due to the powerful low-frequency signals used in this system.
[95] Androjna, A., Brcko, T., Pavic, I. & Greidanus, H. "Assessing Cyber Challenges of Maritime Navigation", *Journal of Marine Science and Engineering* (2020), pp. 11-13.
[96] Walter, T. & Neish, A. "Securing GNSS – A Trip Down Cryptography Lane" in *Inside GNSS* (2020).
[97] Hambling, D. "The U.S. Navy's New Unhackable GPS Alternative: The Stars", *Popular Mechanics* (2021).
[98] Kessler, G. C. "Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity" in *TransNav* (2020), pp. 279-286.
[99] Caprolu, M., Pietro, R. D., Raponi, S., Sciancelepore, S., & Tedeschi, P. "Vessels Cybersecurity: Issues, Challenges, and the Road Ahead" in *Qatar National Research Centre* (2020), p. 6.
[100] Litts, R. E. "Security Improvements for the AIS" in *Old Dominion University Digital Commons* (2021), pp. 31-33.
[101] Defence in depth regards perimeter defences such as firewalls as insufficient since they cannot cope with insider threats. According to the IMO's guidelines, defence in depth encourages a combination of (1) Protection of networks, including effective segmentation, (2) Intrusion detection, (3) Periodic vulnerability scanning and testing and (4) Procedures regarding the use of removable media and password policies, amongst others. For point (1), Boston Consulting Group suggests adopting "more complex cyber protection concepts" such as a zero-trust architecture which assumes every user, device or application interacting with the network is a potential threat. This strategy involves segregating networks and providing a controlled environment that monitors connections in and out of the network.
[102] Chan, S., Yehuda, E., Schaefer, R., Schneuwly, A., Zicherman, S., Deutscher, S., & Klier, O. "Navigating Rising Cyber Risks in Transportation and Logistics" in *Boston Consulting Group Publications* (2021).
[103] Lockheed Martin. "Gaining the Advantage – Apply Cyber Kill Chain Methodology to Network Defense" in *Lockheed Martin* (2016).
[104] The IMO believes that "these rapidly changing technologies and threats make it difficult to address risks only through technical standards". Instead, IMO recommends "a risk-management approach that is resilient, holistic and flexible", one that focuses on being in continuous evaluation against threats and hence the overarching importance of a culture of cyber-awareness. To reiterate, the culture/mindset shift here is recognising the need to move beyond cyber-security as mere annual audit for organisations, and instead have it as an integral and continual activity over time.
[105] Across shipping companies, ship crew, port authorities and personnel employed at ports, organisational culture needs to evolve from one that downplays cyber-attacks to one that recognises the urgent need to address these attacks. The importance of culture in the fight against cyber-attacks is echoed by Captain of the Port of New York and New Jersey, USCG. He believes that the maritime industry needs to recognise cyber-risk management as a "strategic and operational imperative to be managed and championed at the C-suite level and down to the last crew onboard ship instead of an administrative function or a cost-centre".
[106] Tama, J. P. "Trouble Underway: Seven Perspectives on Maritime Cybersecurity" in *Atlantic Council* (2020).
[107] At present, port authorities such as Singapore's MPA are merely echoing IMO's guidelines and requiring ships flagged in Singapore to "demonstrate that they have appropriately incorporated the five functional elements to address maritime cyber-risks. This suggests that current regulations are at best qualitative.

[108] Established in 2009, the IFC is a regional MARSEC centre hosted by the Republic of Singapore Navy (RSN). The centre aims to facilitate information sharing and collaboration between its partners to enhance MARSEC. The IFC has been at the forefront of providing information to cue responses for the full range of MARSEC threats including piracy, weapons proliferation and maritime terrorism. To date, 24 countries have deployed their International Liaison Officers (ILOs) to the centre and they include Australia, Canada, the US and the UK and regional countries. The IFC has established linkages with 97 centres in 41 countries and is potentially well-positioned to include maritime cyber security as part of its ever-expanding mandate.
[109] Today, the Maritime Port Authority of Singapore has in place several one-day courses "for maritime personnel to enhance their knowledge in managing cyber threats and challenges". These initiatives could be expanded on to convey the urgency of improving maritime cyber-security training.
[110] Maritime cyber-security has been in the minds of regulators, although it only came into mainstream awareness and with greater international guidelines following cyber-attacks on Maersk in 2017.
[111] Herr, T. "Trouble Underway: Seven Perspectives on Maritime Cybersecurity" in *Atlantic Council* (2020).
[112] Many large IT companies have programmes in place to reward "bug hunters" who identify vulnerabilities for a fee. For instance, the highest bounty paid out for a security vulnerability found in Apple's firmware is US$200,000.
[113] ReCAAP is the first regional government-to-government agreement to promote and enhance cooperation against piracy and armed robbery against ships in Asia. Its information-sharing centre is based in Singapore and has been credited with increasing maritime awareness against attacks in the region and beyond.
[114] The federal government of Australia recently announced a new law that requires businesses hit by cyber-attacks to report the incidents to federal authorities.
[115] Morgan, C. "Cyber Attacks: The Challenge of Attribution and Response" in *Digitalshadows* (2021).
[116] European Union. "EU Imposes the First Ever Sanctions against Cyber-attacks", Council of European Union Press Release (2020).
[117] SolarWinds is a major US IT firm that supplies software to large corporations and the US Government. They were subjected to a cyber-attack which in turn was thought to have exposed data from these corporations and governmental entities including the Department of Defense and the White House.
[118] Rundle, J. "Letting Businesses 'Hack Back' against Hacker is a Terrible Idea, Cyber Veterans Say", *The Wall Street Journal* (2021).
[119] Androjna, A., Brcko, T., Pavic, I. & Greidanus, H. "Assessing Cyber Challenges of Maritime Navigation", *Journal of Marine Science and Engineering* (2020), p. 11.
[120] European Cyber Security Organisation. "Cyber Security for Road, Rail, Air and Sea" in *ECSO Transportation Sector* (2020), pp. 26-27.
[121] Kramek, J. "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities" in *Foreign Policy at Brookings* (2013).
[122] An increased automation onboard ships which ultimately reaches full autonomy and/or becomes remotely controlled unmanned vessels transporting critical goods across the globe.