Maritime Cybersecurity in the South Baltic Sea

State-of-play, scenarios and roadmap. SECMAR Research report 2021

Spaniol, Matthew J.

Publication date:
2022

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (APA):
Spaniol, M. J. (2022). *Maritime Cybersecurity in the South Baltic Sea: State-of-play, scenarios and roadmap. SECMAR Research report 2021*. SECMAR. https://www.bluesciencepark.se/secmar/a-cyber-security-strategy-for-the-maritime-industry-in-the-south-baltic-region-has-been-developed/

Maritime Cybersecurity in the South Baltic Sea

State-of-play, scenarios and roadmap

SECMAR Research report 2021

EXECUTIVE SUMMARY

The cybersecurity landscape is evolving, driven by a reinforcing feedback loop of increasingly sophisticated attacks and defences. Threat actors, long benefitting from the asymmetrical "attacker's advantage" of focused targeting, have now matured their organizational structures to facilitate tactical information sharing, technique specialization, the establishment of markets for buying and selling exploit and vulnerability information, and providing training on how to circumvent detection and defence systems.

Meanwhile, cyber defenders are tasked to provide holistic protection against unspecified future attacks on rapidly expanding systems. Efforts, resources, and information are much more diluted and much less shared. The cyberdefence community has developed non-commercial forums and means to share information, however, but these relate to identified and publicly shared vulnerabilities. Knowledge of cyberattack specificity is now considered by the private firm as an asset that provides an advantage over rival firms[2]. The net effects are unevenly dispersed threat detection capabilities of companies, blind vulnerabilities, and a steady stream of financially devastating and operationally crippling attacks.

Efforts to bridge these gaps[1] seem to have been counterproductive in the short-term, as threat actors have accessed valuable information and knowledge that has allowed them to concentrate their efforts on high-return exploits from newly uncovered vulnerabilities and zero-day exploits.

SECMAR is an initiative of the EU-Interreg Baltic Sea Programme, whose mission is to advance secure digitalization for sustainable maritime transport. This report is a product of Work Package 3 (WP3); a foresight exercise, whose mandate is to provide a roadmap and strategic recommendations for enhancing and upgrading maritime cybersecurity in the South Baltic Sea Region. The report was generated through desk research, interviews with cybersecurity experts, and cyber-wargaming activities with SECMAR partners and experts.

This report arrives at strategic recommendations by first providing a general assessment of trends in cyberattacks and cyberdefence and mapping those onto the digitalization trajectory for maritime. A set of scenarios is then offered to provide an assessment framework across a range of strategic options to build and upgrade South Baltic Sea maritime cybersecurity competencies. These options are organized into pathways for making the region robust against cybercrime, becoming thought leaders in the field, and designing an infrastructure for developing cutting edge products and solutions.

This report was published in 2022. The report and its content neither represent the policy nor point of view of the EU, nor that of the funding organizations. The authors wish to thank Interreg VB South Baltic Sea Region Programme and national funders for financing the SECMAR project as well as all the project partners and interviewees for their valuable contributions. We kindly ask you to respect copyrights and not to reproduce content without permission from the authors.

[1] for example, driven by organizations or projects such as CISA, NIST, OWASP and others.
[2] for example, in terms of endpoint attacks.

1. INTRODUCTION

The maritime industry is responsible for the transportation of over 90% of global goods. To ensure cost competitiveness and reliability, maritime companies have been investing heavily over the last two decades to upgrade their digital capabilities, connectivity, technology, and systems. This investment has generated a significant return for shipowners, who have been able to reduce fuel consumption and operational expenditures, improve cargo planning and handling, safety at sea, and fleet optimization. The investment has led to dramatically expanded IT systems onboard, onshore, and on cargo. These are generating and leveraging growing amounts of data, which, in turn, is being processed to change the decision-making paradigm away from the captain to a networked one: Everything about how vessels are operated, routes navigated, machines maintained and manoeuvred, cargo tracked, and passengers accounted for and serviced. Networked systems connect cargo to ports to ships to offshore infrastructure; meanwhile, IoT devices are connecting the subsystems in the engine rooms of the vessels, or turbines on the offshore windmills and energy parks. The trend is clear: Everything that can be digitalized will be.

Digitalization investments have demonstrated their value for maritime, and the challenge has turned to interconnecting, modularizing, and interfacing the technologies, systems, and practices. Modular systems, by definition, are interfacing with various other systems. When novel interfaces are developed by joining two or more sub-systems, the security interface requires a custom envelopment. As each system is connected, the cybersecurity defence systems require that the entirety of the connected system to be protected. Not only must each system be cybersecure, but also the connections to other systems and shared services.[3]

Integrating systems, networks, modules, and IoT devices increases the surface exposure of the network exponentially, and security gaps between vendor networks are only identified and addressable by having an overall view of the system. But it remains that the multiple systems providers lack critical collaboration and coordination beyond system installation, and vulnerabilities are increasingly exploited along these modular fissures. Increasingly integrated industry players depend on the cyber-security prowess of all their networked suppliers and providers, which, in turn, is subject to the "weakest-link" principle: If the cyber-security efforts of a single supplier are low, then the risk of a supply chain attack is higher. Given the increasing complexity and specialization of technology, the demands on system providers to identify and address cybersecurity issues affecting their products and development process stop when the discussion rises to network levels. Technologies are well-protected and maintained by their individual manufacturers, but they are a fabricated patchwork, and depend strictly on the scope of their agreed upon contracts. Again, and unfortunately, it is at the interface "bubbles" where vulnerabilities are exploited by threat actors, making it difficult to hold providers accountable.

Meanwhile, cybersecurity remains an afterthought: First connect, then protect. Cybersecurity professionals lament that security issues are considered ex-post, rather than being designed alongside new systems. Older systems - which run the daily operations of critical infrastructure - require considerable attention to continuously maintain, upgrade, and retire.[4] Meanwhile, other parts of the system evolve in different directions: As systems integrate, complexify, and evolve, software itself becomes outdated. Many of the functionalities that are built into a system remain under-used or become redundant. Left alone and unmaintained, outdated and unused code becomes part of the surface exposure. The net result of this is a complex patchwork of cybersecurity with leftover surface exposure due to outdated and long forgotten-software code.

[3] for example network time clocks.
[4] See Faerber, F. The Open Secret-A Shared Legacy. Global Security Alliance. Accessed 25 Jan 2022.

Compensating controls are increasingly required when production runs and/or a lack of institutional knowledge require keeping outdated code in play.

Ships are complex meta systems with 20-30 year (or more) lifespans that can be conceptualized in numerous ways: As a floating well or pipeline (oil & gas tankers), as a floating parking lot or bridge (especially in the case for ro-ro (roll-on roll-off) vessels), floating cities, hotels, or amusement parks (in the case of cruise ships), and more. No two ships, even of similar class owned by the same operator, are ever identical: System configurations and operational software packages are unique to a particular vessel because construction of a complex vessel takes years to complete and many lessons are often learned along the process. Given the unique profile of every ship, local, customized, and costly cybersecurity protections are required, many of which the non-standard are limited to basic, quick-fix solutions at the expense of quality protection. Or left undone.

Until recently, vessels have operated on the open seas where connectivity is limited and unreliable. Vessels were considered, for the most part, offline. However, operations are not only increasingly using - but are increasingly dependent upon - connectivity.[5] Improved global internet coverage, currently driven by private companies, is expanding high-band / low-latency connectivity - eventually covering the vast open oceans and encroaching upon the last nautical mile. Keeping vessels offline or disconnecting a ship from the internet may have been a temporary solution, but over the long-run, is less a feasible option for the global fleet of competing commercial vessels - especially as many equipment vendors require remote access to monitor, maintain, and ensure their systems are operating correctly as defined in their contracts. In the end, access to performance monitoring data of the vessel is crucial for operational efficiency and reducing costs that provide ship operators their competitiveness. In lieu of taking them offline, the correct use of network segmentation, zones and conduits are essential.[5] Perhaps an even stronger driver for the future are the expectations of cargo owners whose customers increasingly require transparent, real-time position and location tracking of their goods along the logistics chain, for example, on platforms using Autonomous Information Systems (AIS) data.[6] An implicit trust in cargo endures in maritime: the cars, liquid bulk such as crude oil and chemicals, fertilizers, and millions of containers shipped every year through and around critical infrastructure rely on orchestrated integrated networks.

Tracking and monitoring of cargo will drive intermodal connections: Warehouses to lorries to vessels to ports to rail to lorries again, and onto the final destination. Connectivity integration across the transport and logistics chain thus requires intermodal data transfer and tracking transmitted across different devices. Invoking IoT into this chain open up systems at various points, resulting in increased surface exposure of assets and infrastructure. As the many different cargos and passengers request connectivity permissions to integrate, service providers face challenges managing the diverse protocol and digital certificates that want to connect and transfer data.[7] While wireless communication protocols (e.g., 802.11) have a standard way of communicating and encapsulating underlying data, different devices with different operating systems are still accessing different applications for different purposes.[8] Meanwhile, companies are reluctant to share cargo information (the critical edge in operational efficiency) and so need to protect cargo and assets from unauthorized access requests.

To reduce the complexity of information sharing in maritime and logistics chains, policy measures such as the standardization of data file formats, are being called for. However, even modest progress on policy has been slow to develop. Instead, as in many cases, policy- and standard-making efforts lag industry development: To protect themselves and their customers' cargo, companies often run ahead of legislation and develop proprietary solutions based on their local experiences. This results in diverging systems (and corresponding cybersecurity protocols, certificates, and practices) that become increasingly sophisticated and thus difficult to translate across industries. Meanwhile, major software providers develop their own solutions that often require specific software to be run on non-compatible systems. In maritime policy, there has yet to be established any mandatory minimums and/or fines for non-compliance in maintaining

[5] The Japanese bulk carrier Wakashio ran aground on a coral reef off the coast of Mauritius in 2020 and spilled 1,000 tonnes of oil. Interviews of the crew indicated the ship was sailing to get a stronger Wi-Fi signal. This motivation remains contested. See https://www.reuters.com/article/uk-mauritius-environment/mauritius-arrests-captain-of-stricken-japanese-oil-tanker-idUKKCN25E1W5?edition-redirect=uk Retireved 10-Dec-2021.
[5] See IEC 62443
[6] See marinetraffic.com
[7] Consider a port's Wi-Fi system at the moment when a cruise ship comes into range, whose thousands of passengers have all been without internet for the last 24 hours.
[8] Consider a container vessel in the future with thousands of containers drawing near a port, and all the containers attempt to communicate with their home office, as well as all of the other containers and assets in their network that are already at the port.

cyber-security. But there are signals that this is changing. In the US, energy and critical infrastructure sectors (such as ports), new regulations are expected to be introduced, for example, in SBOM (Software Bill of Material) management, which proposes an effective way to demand "quality" (and thereby enhanced security) from an industry (such as IT) which traditionally has had little, or none.

In the ports and other critical infrastructure such as offshore energy hubs, the human factor and physical perimeter security systems are also evolving. But local practices diverge and are implemented in non-uniform ways, and in many cases, security checks are still deemed substandard and unevenly enforced. Information about- and attention to- best practices is a necessary precursor. Furthermore, this is insufficient for effective human factor and perimeter security as local cultures and practices remain the key to effective implementation. Less than 5% of containers are ever inspected at ports, and these are not done with digital tools, and the risk that compromised or infected cargo becomes weaponized poses a real threat.[9] Weaponized cargo may remain undetected as it travels across modules, making the carrier the delivery mechanism- and even the medium- of the threat.

Whether implicit or explicit, cybersecurity implementation comes down to a risk-cost-benefit analysis. Installation of new hardware most often occurs in a short window of time while at port. Therefore, maintenance and upgrades may often be rushed, resulting in solutions that lack integrity and suboptimal interface design. Another major challenge is the training of the workforce who need to operate the systems, and the complexity of the numerous tasks and skill sets of the crew are not easily aligned as advancing systems require increasingly new knowledge and willingness to constantly learn new practices and the discarding of past efforts, investments, and work, of legacy systems. This is a driver for retaining the responsibility of vendors for monitoring and connectivity remotely. While the human factor remains the cause of 95% of ship casualties--often due to preventable conditions such as fatigue and distraction--crew and captains protest the installation of new systems and automation and prefer those existing systems be improved instead. Hence, the push for automation and integration of systems is necessary for crew well-being and work satisfaction. Even then, when systems engineers come onboard, the (unique) vessel's specifications do not match the detailed designs, which means that solutions need to be improvised and cobbled together, resulting in suboptimal- or even substandard- solutions.

The report continues as follows: In the next section, we zoom out to review the trends of cybercrime and cybersecurity and then return to issues of digitalization in maritime before presenting a set of scenarios and an analysis of their implications and put forth a roadmap for a cybersecurity strategy for the South Baltic Sea Region.

[9] On balance, some roads, and tunnels (for example the Chunnel tunnel), ion sniffing devices are used to detect explosives in vehicles.

2. ATTACKER TRENDS ACROSS INDUSTRIES

The trends in cybercrime are multifaceted. Below are some that point to the evolving risk landscape posed by cybercriminals, covering 1) Enabling technology and capability trends, 2) Organization trends, and 3) Attack sophistication.

2.1. ENABLING TECHNOLOGY & CAPABILITY TRENDS

Readily available weaponized software

Cyber-security research communities around the world are motivated and competitive about discovering and publishing their findings of vulnerabilities and weaknesses in various IT systems known as PoC exploits (proof-of-concept). Subsequently, these exploits are converted into weaponized software packages, such as the well-known examples are Mimikatz.[10] Likewise, IT security tools such as Kali Linux can be utilized with malicious intent. The open-source availability and instructions for use of such software is available on DarkNet forums, significantly lowering the entry barriers for engaging in cybercriminal activity.

[10] Mimikatz is an open-source application that allows users to view and save authentication credentials like Kerberos ticket.

Improving anonymity and untraceability
Anonymity and untraceability are increasing and being enhanced through more dynamic VPN tunnels, TOR, ProtonMail, crypto-messengers, and other end-to-end encryption. These decentralize the source, making it harder to perform forensic investigation. Without the anonymous feature of cryptocurrencies, ransomware is not easy to implement. Financial payment in cryptocurrencies offer criminals a reduction in the chance of apprehension and raise a sense of security that further lowers cognitive barriers.

Misused technology
Cybercriminals often use familiar technologies to deliver attacks and commit cybercrime: Cloud computing such as Google Cloud and Amazon AWS are being used as "command and control" points for malware. Cloud-based storage systems such as Google Drive® and DropBox® are being used to deliver infected attachments for phishing emails. Some features of the global DNS system are used to deploy scam websites and deliver phishing emails. Infected IoT devices are being used to build botnets that will deliver phishing attempts, host fake websites, and mobilize other threats.

Open-Source Intelligence (OSINT) tools
Cybercriminals use data sources including social networks, stolen data, and special techniques to inquire about potential agents and victims in the development of socially engineered attacks. A good example of this is Shodan, which allows one to search for internet connected industrial controls attached to the internet.

Darknet
Cybercriminal communities share, sell, and rent their knowledge and assets in a semi-criminal way by using web sites in the TOR network that represent the Darknet's neural network. In other words, Darknet is a combination of financial and anonymous IT technologies and human efforts that exist in a distributed way without having an individual leader or coordination locus.

Quantum computing
Quantum computing is evolving at a faster pace than anticipated by any past expert opinion on the subject. Most major world regions (US, Europe, Asia-Pacific) are advancing investment plans, capabilities, and quantum technology Minimum Viable Products (MVPs), be it on the hardware or networking side, with software quickly evolving and the object of vibrant R&D. The first small-factor, room-temperature commercial products are now available,[11] the basis upon which the "single point-of-failure" current TCP-IP based and non-BFT compliant internet, derived from ARPANET, and including all the mainstream cloud tools we use on a daily basis, may eventually decay or be phased out and disrupted by a BFT-compliant P2P/DLT multi-net, which may not require blockchain protocol as it would be natively anti-eavesdrop. Because there is no evidence of any attack using quantum computing, this technology remains speculative.

2.2. ORGANIZATION TRENDS

More information sharing
While once it may have been possible to characterize the cybercriminal as a "lone wolf" operating in isolation, improving anonymity and untraceability allow for increased information dissemination, processing, and collaboration, reflective of organization.

[11] Quantum Brilliance, 2021. https://quantumbrilliance.com/ retrieved 07-Dec-2021.

Improved organization of cyber criminals
Cyber criminals share information, resources, and organize multifaceted killchains in collaboration, and are increasingly planning, consolidating, coordinating, and co-delivering attacks. Organizational effectiveness attracts financing, making activities run for longer periods of time, increasing the duration that an attacker can be active. Unsuccessful attackers, acting individually, may not be able to learn fast enough to retain an advantage, and as defences and detection improves, and the risks of capture increases until the criminal decides that the potential benefits no longer outweigh the risks.

Increasing fluidity of temporary networked actors
The cyberwar landscape is complexifying with the formation of time-interlaced multilevel webs of threat actor networks. The dominant organizational structure can be characterized as the temporary networked organization, one that emerges and organizes for a specific purpose, and disbands once that purpose has been fulfilled. Then, fluid actors may join other temporary networked organizations for a new objective. Over time, reputations and referrals become important for marketing skill sets for enabling value capture from the operation.

Improved division of labour
Organization leads to division of labour, specialization, and niche competencies. The value proposition of specializing in different facets of cyber-criminality (i.e., intrusion, reconnaissance, lateral movement, protocol spoofing, payload deployment, etc.) allow for specialized skill sets to be contracted and applied on demand. This, then, is the manifestation of labour market principles in which services are competitively priced for the value they provide and the scarcity of the supply of skills.

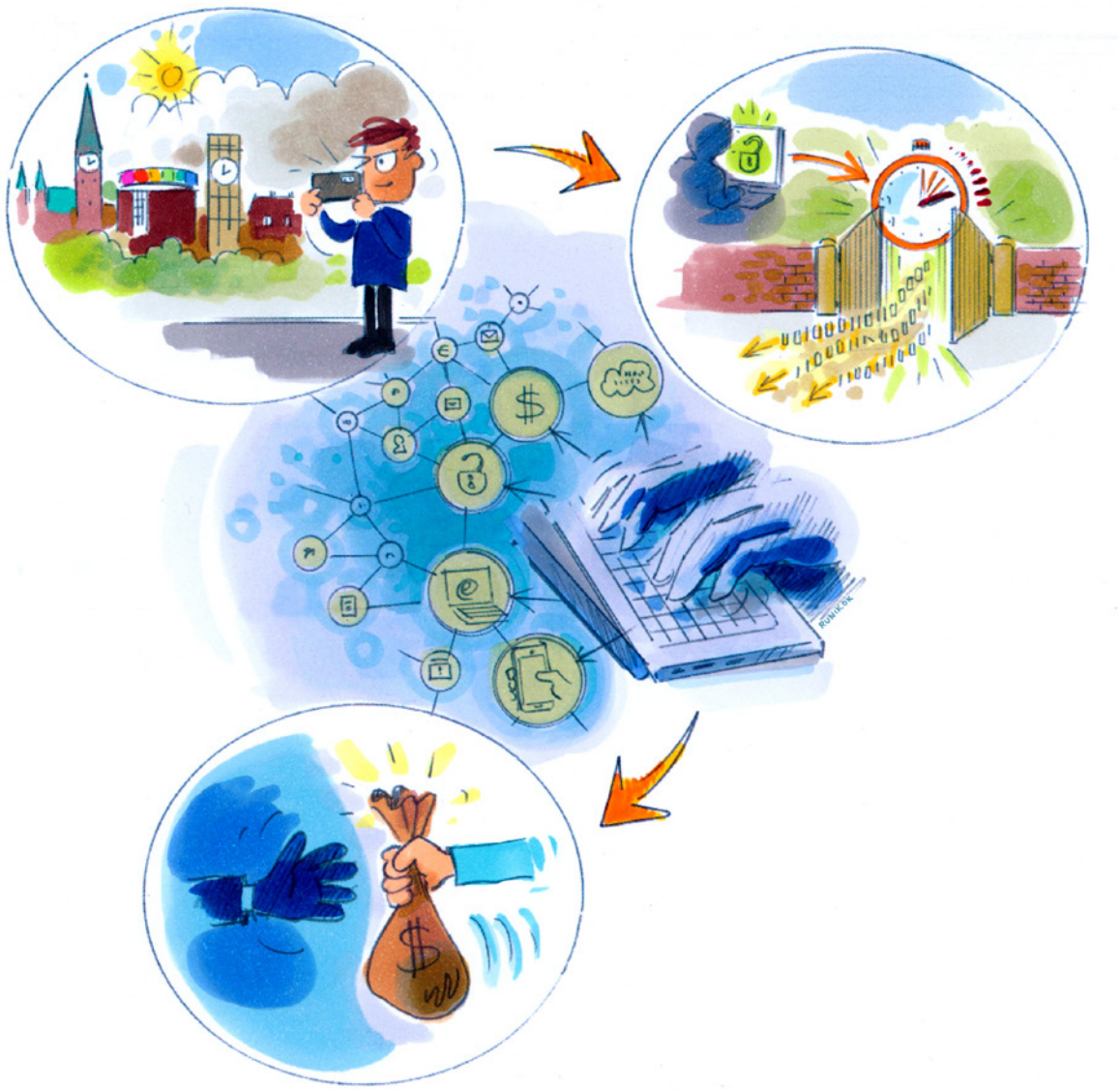
Resource brokering
Actors engage in brokerage activity by arranging transactions between a buyer and a seller for a commission. Brokers may pose non-transparently as a seller or as a buyer, or both. This allows them to procure and recruit products and services on the one hand, and interface with customers or financing organizations on the other. Competing brokers attempt to thwart or reveal the activities of their rivals.

State-supported cybercrime
Analysing and trend-comparing international budget allocations for cyber-security and defence capabilities show an upward spending trend. Civilians and corporates occasionally become collateral damage within this new context. This trend may further alienate governments from their constituencies' interests, and further motivate the formation of secure transborder peer-to-peer socio-industrial cyber defence ecosystems.

In some cases, state actors “capture” cybercriminals in their countries, and convert previously “independent” criminals into agents of the state through threats of violence: Penalties, jail, safety, or the safety of their family members. They are added to the pool of resources from which the state can draw upon when it desires to mount an attack against an adversary. With large budgets and opaque accounting traceability and oversight, states will hide payments to cybercrime brokers for services.

Diverging motivations
Different from the mission- and vision-based organization operating in a competitive market, networked cybercrime is enabled by a diversity of individual motivations: financial, disgruntled, extortion, boredom, addiction, ideological, hatred. Among these, expectations for financial gains remain the most important motivating factor for cybercriminal behaviour. Sums in the hundreds

remain the most important motivating factor for cybercriminal behaviour. Sums in the hundreds of millions have been paid out, and the allure of such paydays - in the mind of the would-be attacker - is the fast track to an early retirement. Beyond financial motivation, so-called “personas” are used to understand the diverse motivations of attackers, especially in crime investigations. Such personas reveal motivations which lead to theorizing for the development of intuitive speculation to seek information that may lead to evidence and the eventual apprehension of the criminal. The motivation of cyber criminality is not in focus in this report because such information does not provide information into the vector, nor is it obvious in its utility for the prevention, mitigation, and remediation of the cyberattack.



Patterns in cybercrime business models.

What: Blackmail; Extortion; Ransom. Who: Sleeper agents; Turning Allegiances; Insider targeting.
Why: Financial; Disgruntled; Ideological; Hatred. How: Gather intelligence; Disable operations; Weaponization.

2.2. ORGANIZATION TRENDS

More surveillance by cybercriminals
Would-be attackers are increasingly “listening on the line.” Any attempt to communicate and transmit information, can in principle, be intercepted. A prevalent heuristic in cybersecurity relates to traffic: If it can be transmitted or communicated, it can be disrupted. Open-Source Intelligence allows cybercriminals to do reconnaissance and identify information that can provide insight on how to develop attacks.

Increasing vulnerability brokering
Combining advanced skills sets and capabilities with external markets, the emergence of vulnerability brokerage markets can be expected to increase. Vulnerability brokering sees information about cybersecurity weaknesses being sold to would-be attackers, or to the financiers or contractors that hire cybercriminals for mounting attacks. Such markets enable and facilitate cybercrime educing transaction costs for employing specialized services.

Increasingly more fradulent mechanisms

- Increasing sophistication of impersonification and so-called “deep fakes”
- Ordering unauthentic "knock-off" parts
- Non-order deliveries
- Payment interception by faked intermediaries

Increasing options for attack vectors

- Weaponization of operational technology
- Weaponization of cargo
- Weaponization of cargo transport

Cyber-attack automation
The increasing number of attack attempts is well documented. Global Internet providers log hundreds of thousands attack attempts per day. These attacks are not, of course, individually programmed and delivered. In such “shotgun-blast” attacks, programs are bundled in packages that are delivered which automate exploitation of known vulnerabilities. Furthermore, such a strategy works to exploit the behaviours of workers. Probabilistically speaking, as more “clickable” opportunities appear on the screens of workers, the higher the total count of clicks on those links, accidental or otherwise.

Faster attack spreads
Once access to a network has been established, defences are mobilized. One way to improve the success of an attack is the “pivot,” or compromising one system and then move laterally across other systems until it is possible to elevate access privileges to a network. This provides multiple avenues and stochastic pathways to improve the run probabilities for success.

3. SECURITY TRENDS

There is a growing acceptance of the fact that all systems will eventually be hacked. As Robert Mueller, ex-director of the FBI said, "[t]here are two types of companies, those that have been hacked and those that will be." As attacks are increasingly more enabled by advanced technology and perpetrated by increasingly sophisticated organizations, the cybersecurity community is responding in-kind across the cybersecurity spectrum, from early system design to the implementation of advanced tools and techniques, new ways of collaborating, increased specialization, and attitude training. With pending inevitability of eventual attack, business continuity and disaster recovery are becoming ever more important. This section reviews developments in evolving security, attitudes, and behaviours.

Digitalization projects that design and engage cybersecurity from the beginning of production to the delivery of products are more secure. As a result, system cyber-security features are considered as a quality component, going well beyond the general conception that regards information security as one-dimensional, for example, “is it password protected?” This trend is recognizable in the advancement of Security Operations (SecOps) or Development, Security and Operations (DevSecOps). These call for integrative measures such as security requirements engineering and misuse case analysis.

Another development is the increasing specialization given the advanced threats posed by well-organized and well-equipped cybercriminals. Firms have long outsourced their cybersecurity to specialized firms and are increasingly abandoning internal IT development departments altogether. These are being replaced by IT contract managers who negotiate services with external providers. By increasing the outsourcing of cyber-security to dedicated security providers, these providers can accumulate knowledge on emerging threats.

Cybersecurity ecosystems have been proposed as an inter-organizational defence community to match the increasing sophistication of cybercriminal organizations. Cybersecurity ecosystems would link professionals together across value networks to defend systems that are increasingly spanning organizational boundaries. In such shared defence systems, professionals can focus their development agendas on those points in their systems of which they are accountable, and then disseminate these across the ecosystem.

IT systems are increasingly protected by automated Intrusion Protection Systems (IPS) or kill-switch systems (which are not recommended for industrial control systems). These monitor integrity and traffic, and at the sign of a breach, can automatically initiate different responses to thwart different threats and attacks. Responses range from collecting incident evidence by system memory dumps, to alerting cybersecurity professionals of suspicious activity, and local-to-full system or network shutdowns. Likewise, tools and methods for catching criminals are improving. At the end of the day, financially motivated criminals must try to cash out the money, and after successful attacks, this is an important moment for detection. This is more difficult if motivations are opaque or agendas are environmentally, ideologically, vengefully (etc), driven.

Such security orchestration, automation, and response (SOAR) systems, commercially available in cloud-based systems, are resulting in improved damage control and faster attack recovery. Provider business models are also advancing. Examples include Security as a Service (SECaaS), Security Operation Centre as a Service (SOCaaS) and Managed Security Service Providers (MSSP). Cyber security vendors offer their service and expertise via diverse models, such as subscriptions, per-hour billing, pay-for-pain removal, and dedicated in-house staffing.

Software code that is developed open source has demonstrated its robustness as it is subjected to the scrutiny of the crowd. For newly developed code, large firms routinely offer more so-called "bug bounties" that financially incentivize programmers to simulate the role of the cybercriminal or peer-review and to discover vulnerabilities early.

Changing mentalities and conceptions about cybersecurity requires ongoing efforts. One example, previoulsy mentioned but worth repeating, is to. is to design systems with cybersecurity in mind and take that along the IT development processes. Another is to assume the breach mindset within a never-ending story of cyber-attacks. Despite the confidence we have for the defensive protections in place, cyber professionals should assume adversaries will eventually find a way to penetrate security perimeters. Such a mentality can be operationalized in various parts of business security programs, such as incident response, business resilience operations, redundancy, and contingency plans. Enterprise Risk Management (ERM) recommendations such as those developed by NIST, or framework proposals such as those from Central Authentication Service (CAS), Control Objectives for Information and Related Technologies (COBIT), ISO 31000[12], Risk Management Society (RIMS), DNV class notation voluntary addition - cyber security DNVGL-RU-ship Pt.6 Ch.5 Sec.21 & others may become increasingly important as they extend to cybersecurity.

So far, cyberthreats have been met with improved security measures. The trend is not toward easier defences to threats, but that the increasing sophistication of attacks warrant increasingly complex solutions. Speculative cybersecurity threats from quantum computing aided attacks are resulting in theoretical defence development. Using dynamic 2-point location on arcs or using crystals have been proposed as possible defence measures, but these need development and testing to be ready and deployable in the case that quantum computing-enabled cyber-attacks begin.

While many of the trends point to positive developments for future cybersecurity, some trends paint a more dismal portrait of things to come. First and foremost is the increasing risk to people

[12] See https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf

given the advancing weaponization of Operational Technology or Industrial Automation and Control Systems (IACS). Human lives are increasingly at risk, and this creates new categories of severity for IT breaches.

Secondly, as cybersecurity increasingly specializes, new languages and jargon are introduced which make communication between firms and vendors and providers increasingly challenging. Miscommunications - specifically to C-Suite of executives - can lead to underinvestment in appropriate protections because they are not sure what they are buying. Vendors often fail to speak the language of the boardroom, instead, habitually using the technical jargon which is not understood outside specialized communities of practice. Meanwhile, the surface exposure of the aging software code presents an additional communication problem, as older code is increasingly opaque as to its function. The workforce that was tasked to code the software of the earlier systems are now retiring in large numbers, and along with them, the knowledge of the nuances of the programs. The result in the growing need for software archaeology--dedicating resources to review older code and systems to upgrade or replace it--which is posed to require increasing attention in the future to re-secure systems that were previously considered safe. This re-focuses attention to the demands for lifetime security planning.

With the rising costs associated with cybersecurity protection and maintenance, many small and medium-sized firms are unable to afford adequate protection and updates, leaving them vulnerable to the eventual crippling cyber-attack. Likewise, there is an increasing need for investment in physical (perimeter) security. Perimeter security can delay or detect people and vehicles from entering secured areas. To this day, the major culprit remains the USB stick, or transmitter hidden inside of a ballpoint pen, which were given as gifts to the trusted employee.

With all the cybercrime, insurance companies are adapting. For those adapting, trends indicate higher requirements, more exceptions (known as “Lloyd’s exceptions”), higher systems maintenance requirements, increasing evidence to demonstrate breach in cases of attack, with decreasing pay-outs and guarantees. Indeed, insurance against cybercrime is disproportionate, as large companies and governments occasionally pay out astronomical sums, while small and medium sized companies are ransomed proportionally. The net result of such imbalance is that insurance companies are limiting their exposure and coverage or discontinue offering insurance against cybercrime altogether: The pay-out of ransoms by insurance companies has all but stopped due to the threat of sanction if the payment is known or suspected to be made to a sanctioned organization or government, which, in turn, risks that the paying company also be subject to sanctions.

Governments are equally strapped to combat cybercrime. Resources are only mobilized in high-profile cases, and little recourse is left for small and medium-sized companies. In some countries, governments are implementing penalties for non-compliance of firms. Such rules drive firms to pay for certification that limit the burdens of auditing. They are then effectively hiring 3rd party cybersecurity auditors and compliance professionals to manage this requirement.

In the end, the cornerstone of cybersecurity involves the human factor. The labour market for cybersecurity professionals faces a shortage of professionals, driving wages and costs higher. In the crowing complexity of the cybersecurity domain, a skills gap has manifested as the need for specialists grows. This situation additionally undermines the academic “credentialing” offered by private organizations who train in specific programming languages and systems. It has been estimated that there is an urgent need to educate 1,5 million professionals, and the urgency also presses the educational institutions to develop students in apprenticeship programs. In the long-run, this may short-change efforts as there are already needs for multidisciplinary approaches to cybersecurity.

4. DIGITALIZATION OF MARITIME

The future vision of maritime is a fully digitalized and optimized one. Sustained investments in digitalization have driven the process for two decades, starting with the introduction of the flowmeter around the year 2000. Today, efforts to process, manage, and visualize the data so that operators could effectively optimize workflows has become the key to competitive advantages, as those investing in digital technology are able to reduce operational costs, crew, and fuel consumption. Various perspectives can be taken on the digitalization of maritime, including onboard ship operations, onshore cargo planning and across the logistics network, ship services such as shipbuilding and repair, and emerging offshore industries such as ocean energy production and other offshore structures such as aquaculture farms.

Onboard ships, digitalization covers many facets such as route optimization, fuel consumption management, predictive systems to inform maintenance, service, and repairs (including hull and propeller maintenance), cargo stowage, and ballast optimization. These operational activities require the generation of data, which is transferred to home office for data analysis and planning.

Onboard optimization achievements are enabled by the increasing utilization of Industrial IoT devices. Vessels are producing ever-increasing amounts of data thanks to the introduction of onboard technologies, sensors, and cameras. An increasing amount of this data is being generated and managed by 3rd party providers who ensure that data and services are leveraged as contracted. Indicative trends - such as the adoption of IPV6 increases - point to a future where every device may eventually have its own IP address. Indeed, connectivity is becoming a competitive advantage (especially for charterers), who can deliver reports and updates to their customers. These companies thus have an ideal for 100% reliability in connectivity so they can meet these expectations of their customers.

The critical bottleneck remains in the processing of this data--most is still analysed by land-based offices. Thus, the effective management of the fleet requires increasing bandwidth to be able to transmit said data. However, much of this transmission is still not even possible because of the lack of connectivity on the open oceans. This is set to change in the not-so-far future. Plans for increasing connectivity at sea by expanding the coverage of satellites is on the roadmap of many developers. These will increase the speeds of transmission of data, that at one point in the not-so-distant-past, was done in the once-a-day noon reports. Marine 5G via satellite networks at sea will bring ships online with fast connections, making them easily identifiable by criminals and opportunities for attacks.

These bottlenecks pressure others in maritime value chain to accelerate their digitalization efforts, shaping the supply chain toward integrated logistics. Data about cargo position, condition in terminals help shorten port calls. Leveraging real-time cargo data throughout the supply chain opens for improved coordination. However, this integration comes with a security risk. Shipping companies do not have control over their service suppliers and must trust that they have implemented effective cybersecurity protocols and practices. As the old Arab proverb says, “[t]rust in god but tie your camel first.” Meanwhile, ports and repair yards are investing heavily in their own digitalization journey, for example in the automation of terminal tractors, lifting machines, and cranes, to improve operational efficiency.

Developments in AI, machine learning and machine vision are beginning to find their way on-board ships and in the processing of ship data. While research and development of these technologies have come far over the last decade, a shortage of IT workers seems to have slowed their implementation. This could perhaps become part of the threat landscape, as these may be sensitive to manipulation, for example, by spoofing data in a way that projects a new course or behaviour in an automated system.

DIGITALIZATION OF MARITIME

5. SCENARIOS: MARITIME IN 2035

Scenarios are future-oriented thought experiments that describe a series of plausible operating contexts in which an industry may find itself. The scenario narratives can be used to stress-test business strategies and policies. They are built upon an exploratory analysis of critical uncertainties toward the year 2035. The two uncertainties used to develop the scenarios in this report were 1) maritime industry cohesion, and 2) the character of global economic growth.

Industry cohesion captures Maritime's ability to deal with challenges jointly. Examples of challenges that the industry can collaborate on include reducing emissions regulations in the face of climate change, the integration of international standards for technology. But the question remains, to what extent will the industry pull together to make joint solutions and a level playing field for healthy competition?

The second uncertainty is the question of economic growth. At the time of this report, there is a concentration of wealth into the hands of few large corporations and private individuals. The COVID-19 crisis seems to have exacerbated this problem. On the other hand, there is a long-term trend of inclusive growth coming from a swelling global middle class. While these are not necessarily mutually exclusive, the character of the future of economic growth provides frameworks for speculating about how developments many occur, which are made salient in the scenarios below.

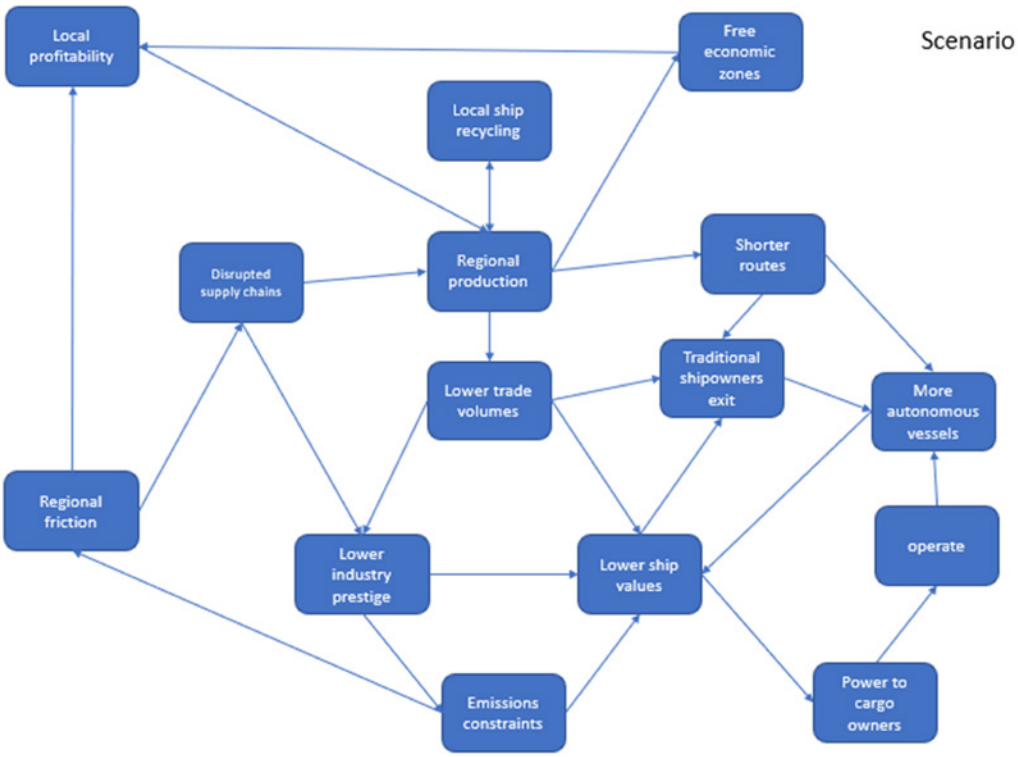
A) INDUSTRY COHESION AND POLARIZATION
Scenario A: Sprint

Supply chain crisis of late 2021 leads to fast growing 3d printing activities and automated manufacturing in the region. At first it was just critical parts and spares, but it quickly grew to cover many stocks and segments. Deep sea trade for goods, metals, cars, is being threatened and disrupted, as does demand for warehousing and port activity. Fossil fuels such as coal, oil, and gas are being phased out and the EU ship taxonomy made it more expensive (financially and for insurance) to be in businesses which are not taxonomy friendly, as the EU pushes for CO2 targets and taxes at any cost.

Shipping gets more regional as friction grows between regions. Production is moved back into free economic trading zones in Europe as trust in China, Russia, and Asia drops. China cuts off much of its diplomatic activity as it turns inwards to focus on domestic issues. Trade forecasts drop, which lower the prices of ships, down to the price of their steel for ships on the routes that cease to exist.

Aging family shipping firms struggle as rebuilding ships to taxonomy became too expensive and there are difficulties passing firms through to the next generation as the challenges seem to be too large to overcome and not worth the effort. Paying CO2 taxes, obligations to recycle ships at the end of their life cycle and moving their banking businesses outside of the EU.

Scenario A: Sprint



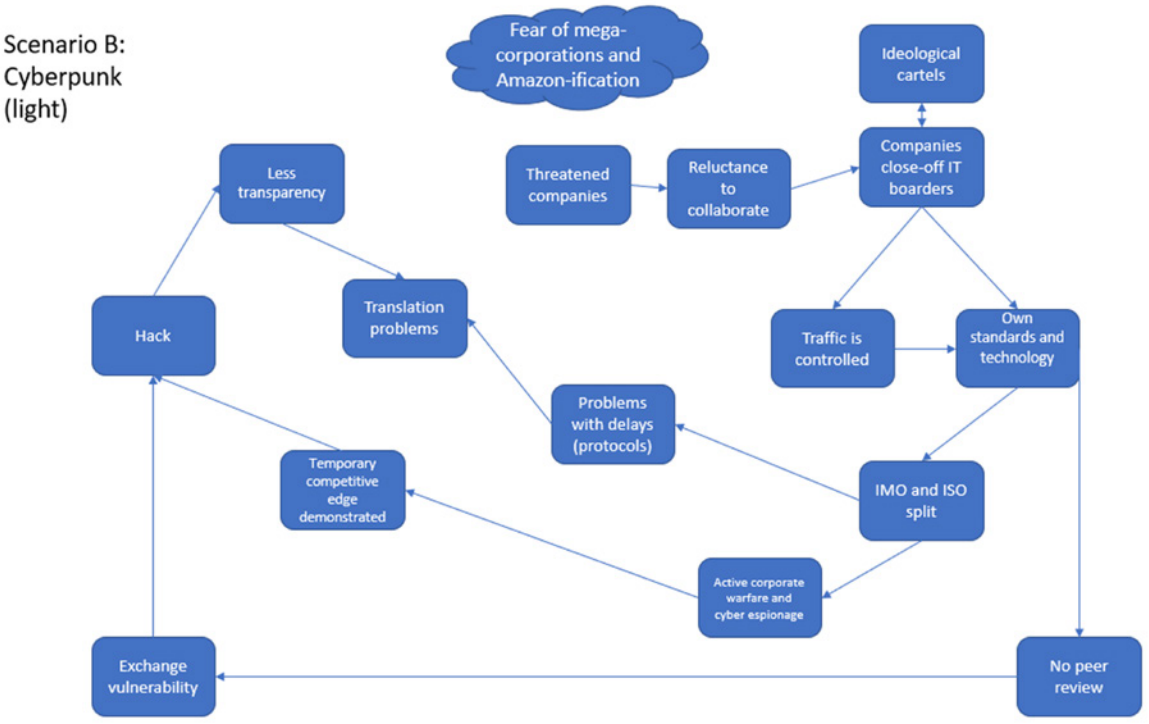
B) INDUSTRY FRAGMENTATION AND POLARIZATION
Scenario B: Cyberpunk (light)

Mega corporations are using their negotiation power to threaten to squeeze shipping companies. Companies are responding by closing and walling off around their supply chains. Collaboration among shipping companies declined, and supply chains, to protect themselves, began to adopt their own standards and protocols.

Uneven standards caused fissures in the industry, leading to deeper fragmentation. Peer and open review ended. Translation between independently developed protocols increasingly caused delays. Other protocols were simply rejected.

Nations also begin to adopt these standards for the companies doing business in their geographical domain, leading to less competitive markets, and increased political barriers to trade. Cybersecurity became a key component across competitors, and industrial espionage and sabotage became increasingly common to gain a competitive advantage by controlling traffic and persuade legislators to fall in line with the big corporations.

Geopolitical and ideological cartels solidified, who consolidated their power to force their standards across nations and industries. The cybersecurity standards arms race became the key to competitive advantage- albeit only a temporary one, as predatory attacks reversed these advantages over time, which found and exploited weaknesses at data exchange interfaces.



C) INDUSTRY FRAGMENTATION AND GMC GROWTH
Scenario C: Amazonification

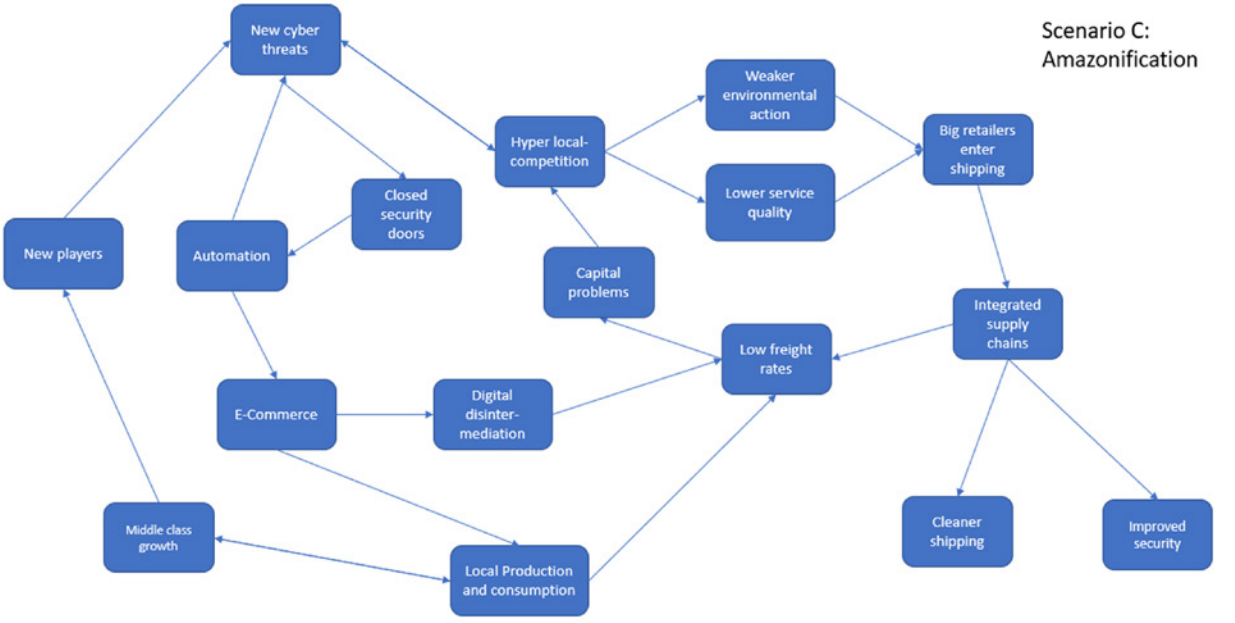
The shipping industry is plagued by heavy competition on a cost basis, resulting in failure to deliver on service, environmental standards, and still the costs, that major customers like Amazon and IKEA demanded. This prompted large retailers to invest in logistic assets - beyond just chartering - and thereby enter into direct competition with the traditional shipowners. New ships, operated by big retailers, have been able to reduce their freight rates by 50% by taking firm control and security of the supply chain.

The industry fragmented in their struggle to obtain capital and made competition even more fierce. In desperation, traditional shipbuilders order a new fleet and put new capacity on the water, lowering freight rates even further.

Growth in global consumption grows the African middle class, but the rise of e-commerce platforms, deep digital disintermediation, and local manufacturing prompts shipowners to increase their cyber surface exposure, including in their port networks. Cybersecurity threats plague the traditional shipowners. Rumours have it that even shipowners are exposing weaknesses of their competitors' cybersecurity, leading to increased mistrust and fragmentation. Shipowners try their best to defend but are ultimately forced to remove their assets and operational knowledge from the cloud and put it back onboard the ships, who cut all connections to the Internet.

Regional ship management companies abandon the traditional players and choose to work for the retail shipowners who force them into non-compete clauses.

Scenario C:
Amazonification

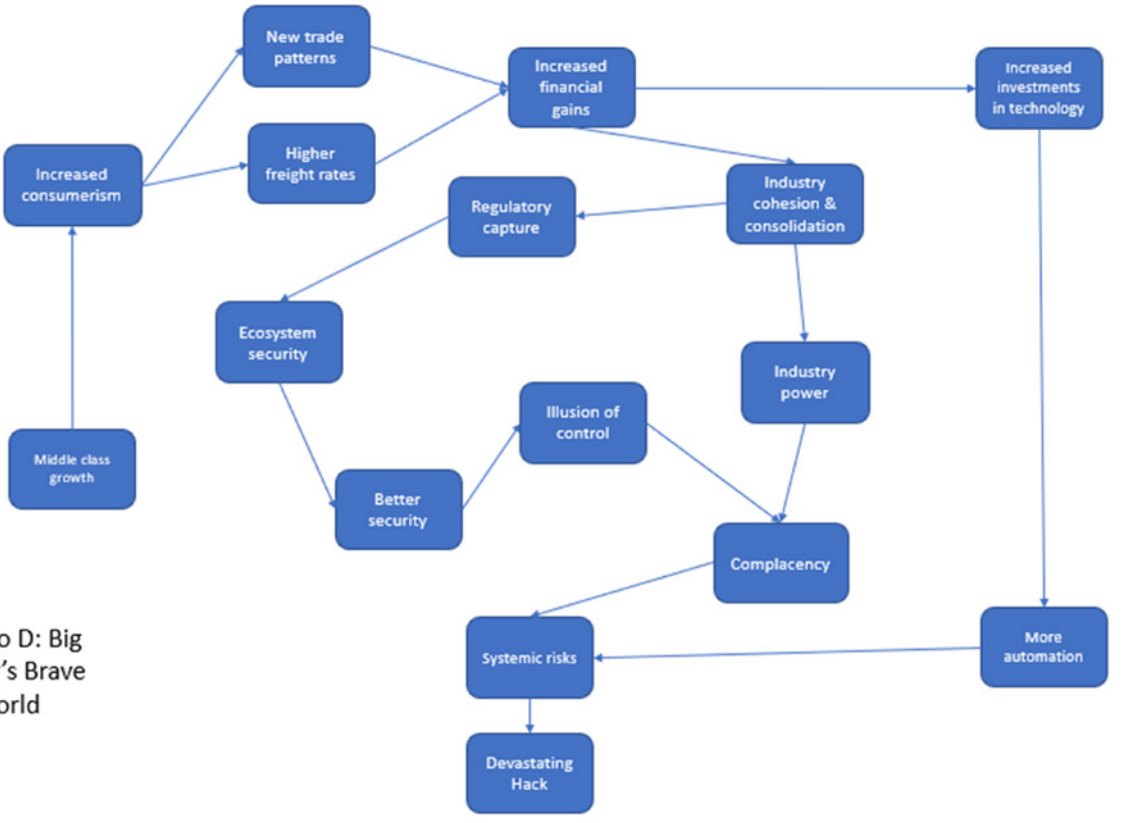


D) INDUSTRY COHESION AND GMC GROWTH
Scenario D - Big Brother's Brave New World

A growing world economy will drive new consumer behaviours and trade patterns: environmental concerns will lead to greater consumer awareness of how their collective wallet might positively impact CSR (Corporate Social Responsibility). This will translate to higher demand for more sustainable practices such as greater levels of g/localization and increased market requirements for certified goods provenance and ethical production. Demand for long route logistics will subsequently give way to an ever-increasing focus on regional and last mile logistics. This shift will be coupled with greater levels of integration between carriers and cargo owners via for example DLT/blockchain industrial ecosystems. These new shared organizational ecosystem models will deliver over many dimensions including enhanced cybersecurity (for example, by integrating cargo cybersecurity with that of vessels and ports, as well as greater resilience against organized, distributed, and well-resourced cybercrime networks), ability to add value services for cargo owners and end-consumers such as proof of provenance, higher flows predictability and many other benefits.

Meanwhile, dynamic demographics (simultaneously growing and aging population) will drive higher levels of automation, digitalization, and technology adoption. Driven by necessity (not enough workers), this trend will bridge the proportional workforce contraction (millennial cliff) impacting global population until it plateaued circa 2050/60. These demographic trends will extend their impact to M&A activities, as they will also affect the corporate executive and shareholding layers. More industry concentration shall be expected: the cumulative impact of all these trends will be indeed particularly felt in the long-route maritime sector. This will be further facilitated by higher freight rates and enhanced profitability, with financial gains from established firms combined with a greater appetite for acquisition resulting in more takeovers of weaker competitors or younger enterprises, especially those technologically advanced.

This intense industry consolidation of companies and systems will usher another level of globalization. As industry consolidates and becomes more centralized, its combined power will result in a gradual regulatory capture of organizations such as IMO and ISO. While having the initial effect of reducing geopolitical tension and increasing defence capabilities, this concentration of power might ultimately lead to increased complacency. Subsequently, a decaying governance scenario might open the doors to individual hacktivism and the asymmetric exploitation of new system-wide vulnerabilities, leading to unpredictable 0-day attacks, the scale of which might cripple the entire global trade flow, and the world at large.



Scenario D: Big Brother's Brave New World

STRATEGIC PROJECT FOCUS AREAS

To catalyse the acceleration of a vibrant cybersecurity community, two strategic areas are suggested to provide a base for future development: 1) Political action to develop markets and customers who increase uptake of cybersecurity products and services by advancing regulation and standards, and 2) Spurring sectoral motivation for advanced cybersecurity products and services by encouraging the sharing of cyber defence intelligence and the undertaking of training.

POLITICAL

Cyber security standards have been developing over time at the IMO and at standards organizations, but efforts need to be made to accelerate their development. One way to do this is to look across industries (such as to the aviation and automotive segments) for benchmarking best practices. This will open the discussions and agendas for a wider perspective on what can and should be done. In the interim, the US has developed an advanced approach to developing maritime cybersecurity techniques given their expansive fleet of naval ships that can be used as reference for the global commercial and merchant fleets. Organizational and procedural principles should be reviewed as well to streamline the collective development of standards.

Some of the core topics that need to be addressed by standards include:

- Encryption standards
- Software auditing and certificate frameworks
- Data classification schemes for instruments, cargo, and crew

Adequately addressing the topics above would enable cybersecurity practices to transition from a "blacklist" approach (which prohibits substandard practices) to a "whitelist" approach which delivers an approval of practices. While this would be a challenge to implement operationally, such an approach would lay foundations for advanced standard setting.

Another approach that cybersecurity regulators can take is to enable the maritime industry to start protecting itself collectively. Since companies are reluctant to share detailed information about their cybersecurity practices and threat detection intelligence, and patches are dependent on the scope of vendor contracts, creating new markets and incentives to share intelligence can support sectoral awareness. Once cooperation has been established--and elevated to the Security Operations Centre (SOC) level--it is plausible that the industry would be able to develop solutions at higher levels of measurement scope and facilitate the further steps to develop collaborative security systems that can protect the wider fleet community, enabling a sort of ecosystem-based cybersecurity movement to emerge.

Concrete information that can be shared could include:

- Real-time cyber threat detection
- Asset weaponization threat and killchain concepts
- Best practices in patching

A third avenue for policymakers would be support for the development of a think-tank on maritime cybersecurity. This would dedicate itself to a collective intelligence mission and serve as an intelligence clearinghouse at the service of the diverse actors in the maritime community, a structure to gather and disseminate information and support research on emerging issues such as the implications of quantum computing and engagement with "ethical hacking" and the co-generation of solutions. It could develop and test advanced features when new ships are built

to establish their effective in a host of contingencies. It could also provide training in the form of cyberwar gaming and consulting services financed by pooled resources to develop expert solutions to challenges that can be accessed by members, such as a "spellchecker" for security code that actors can use to audit the code of their partners.

SECTORAL

At the sectoral level, several recommendations are made salient in this report. An overarching zero-trust approach to cybersecurity does not exist among the players. This is of critical concern as the extension of high-speed internet will reach vessels once considered “offline.”

Maritime companies remain independent and underprepared and thus vulnerable. Cargo carriers need to ensure vessel, equipment, and cargo integrity, including at the interface of multi-modular infrastructure--at ports and terminals. These require improvements in tokenization and authentication processes such as certificates, certificate frameworks, agreements on system updates, enhanced cryptography, segmentation, (when possible) the phasing-out of legacy communication systems such as e-mail, and outright banning personal electronics. Under the umbrella of a ship-and-asset communication constellation with a shared risk management agenda, a protective layer can serve as a first line against attack.

The sector needs to invest in new technologies and capabilities to secure the ecosystem. Examples include:

- Smart cables that can monitor their own integrity
- Geofencing at critical infrastructure and dynamic geofencing for moving assets
- Red teams properly incentivised to identify unsecure access points

Furthermore, cybersecurity should be designed alongside the vessel: This would help ensure system-wide integrity. They can thus be encrypted, fitted with (legal) honeypots, and wireless redundancy (for LEOs).

Newly built ships offer the chance to radically reconsider cybersecurity-enabled damage control in the case of an attack: Current practice adapts features in hindsight or retrospective consideration. Developing back-up systems might see the development of a “stealth mode” for cloaking vessels, “emergency kill-switches” and “vessel default safe mode reboot” features to mitigate damage in an attack. Even more radical would be the development of cybersecurity alongside digital twins that can be brought online when the primary system is compromised. Today, they are primarily used as “test-beds” but elevating their functionality and being able to replace systems with a twin on “standby” could lower downtime. At its end of service, vessels should undergo a ship recycling cyber check (SRCC).


1.
ECO SYSTEM
CYBERSECURITY
WEAPONS THREATS
COMPANIES COOPERATING SOC
CYBER THREATS
2.
BACK-UP DEVELOPMENT
DATA CLOUD
NEW BUILDS
DATA CLOUD BACK-UP
DESIGN/ DEVELOPMENT
"BOOT"
A
B
DIGITAL TWIN REDUNDANCY
4.
SHIP COMMUNI-CATION
QUANTUM ECOSYSTEM
SHIP RECYCLING CYBER CHECK
PASSWORD
SPELLENCHECKER
CLICK
INVISBLE BUTTOM
ETHICS AND BOUNDARIES


3.
GEOFENDING
PASSWORD
SNIFFING FOR UNSECURE ACCESS POINTS
ROBOT AUTHENTICATION
GOODS - CREW
WiFi
www.domain.com
5G
SECURITY STANDARDS
AVIATION/AVTO/ US APPROACH
WIRELESS REDUNDANCY
PC
NO PERSONAL ELECTRONICS
SOFTWARE SOLUTION AUDITING
5.
CYBER-SECURITY THINK-THANK
ETHICAL HACKING
WARGAMING TRAINING SEMINAR
RUNIK.DK
RESPONSIVE TO CRITICISM AND COLLABORATING IN THE CO-GENERATION OF SOLUTIONS

SECMAR

Interreg South Baltic

EUROPEAN UNION

PARTNERS

BLEKINGE TEKNISKA HÖGSKOLA · BTH ·

MDC The Transport Innovation Network

BLUE SCIENCE PARK

ppnt gdynia

KLAIPĖDA SCIENCE AND TECHNOLOGY PARK

www.southbaltic.eu/-/secmar
www.bluesciencepark.se/secmar-eng/

Contact:
Matthew J. Spaniol, Ph.D.
Matthew.spaniol@gmail.com
+45 5012 6444