Stellenbosch
UNIVERSITY
IYUNIVESITHI
UNIVERSITEIT

forward together
sonke siya phambili
saam vorentoe

RESEARCH BRIEF 10/2023
Security Institute for Governance and Leadership in Africa

SIGLA @ Stellenbosch

Author: Prof B. van Niekerk
(DUT & Research Fellow SIGLA)

Series Editor: Professor F. Vreÿ (SIGLA)

Cybersecurity in the maritime domain: Incidents and best practices

Introduction

The maritime domain carries most of the global trade and is crucial to many economies. In addition to the cargo carried by seagoing vessels between ports, undersea infrastructure carries oil and gas through pipelines, and information is carried via the undersea fibre-optic cables. The importance of these trade routes and the infrastructure makes them attractive targets for state actors and cybercriminals alike.

For the purposes of this brief, the maritime domain will be comprised of three main constituents: the ports, the seagoing vessels, and the undersea infrastructure. The next three sections provide a summary of cyber incidents impacting each of the three maritime constituents. The concepts of critical infrastructure and economic information warfare are introduced in relation to the maritime domain. Thereafter, an overview of best practices and authoritative documents is provided.

Cyber Incidents at Ports

Cyber incidents were reported to have doubled at the Port of Los Angeles from the beginning of the pandemic to mid-2022, reaching approximately 40 million incidents per month. The incidents have been attributed to state actors seeking to cause economic disruption, and ransomware groups seeking to make a profit through extortion. Ransomware can become particularly problematic, with examples of major incidents resulting in operational disruption being Transnet in South Africa and the Port of Nagoya in Japan. San Diego port and the Port of Lisbon also suffered ransomware incidents in 2018 and 2022, respectively; however, operations were not affected. The NotPetya incident, which was attributed to Russia and reclassified as a wiper, is the World's most financially damaging malware, and it severely affected Maersk's operations globally in 2017.

While ransomware incidents are more noticeable, other cybercrime activities (such as business email compromise, phishing attempts, and fake domains impersonating organisations as examples) and cyberespionage (such as the IceFog campaign and system intrusions against the Indian navy to track warships) are still present and can impact on maritime organisations and ports. These types of activities are also potential initial compromises that could result in ransomware or other malware infections. Some ports have experienced system intrusions by criminal syndicates to monitor the cargo where contraband was being smuggled.

Other incidents – possibly unique to the transportation and maritime domains - is spoofing and interference with GPS and the automatic identification system (AIS) on ships. This interference has occurred at ports (for example Shanghai) and has caused navigation issues to vessels under pilotage and automated equipment in the port.

Cyber Incidents Impacting Vessels

Oil rigs have suffered cyber incidents such as system intrusions disabling the safety systems aboard oil rigs, and another tilted an oil rig; malware has infected oil rigs, including impacting the positioning system. Malware has infected Royal Navy warships, the Electronic Chart Display and Information System (ECDIS), a power management system, and onboard business systems (Baltic and International Maritime Council (BIMCO) *et al*). Shipping company DNV's fleet management software was infected by ransomware in January 2023, with an impact on an estimated thousand vessels. In 2018 the vulnerability search engine Shodan implemented a ship tracker, where vessels with vulnerable systems (for example satellite communication) that were exposed on the Internet could be easily found and potentially interfered with remotely.

As described above, interference with GPS and AIS can result in trouble with navigation. Simply jamming the GPS signal will degrade the ability to navigate; however, spoofing a GPS signal with incorrect coordinates can result in vessels or equipment going off course. Spoofing of AIS has occurred, where warships were shown on ship trackers off the coast of hostile countries while they were actually in port.

In addition to malicious actions, system errors reported are useful to illustrate the potential impact of a severe cyber incident related to onboard systems. In one incident, most of the navigation systems of a ship failed in a high-traffic area during a time of low visibility; in another, the navigation systems crashed while the ship was under pilotage.

Cyber Incidents and Undersea Infrastructure

It is estimated that 97% of the global Internet traffic traverses undersea fibre-optic cables. The Insikt Group (2023) and the European Union Agency for Cybersecurity (ENISA), provided reports on the growing threat landscape for undersea cables, namely intentional physical damage, espionage by tapping into the cables, and cyber incidents. In 2022, the US prevented a cyber incident targeting an undersea cable and in 2023, the African undersea cable operator Seacom was a victim of ransomware. The incident was contained in its hosting environment and did not affect the operations of the cable itself. However, a cyber incident affecting a cable landing station, or the network management systems could disrupt services.

Microsoft has experimented with an undersea data centre, which if deployed at a large scale would place more of the global Internet infrastructure undersea. Post-quantum encryption technologies were also tested with the data centre. While secure connections can mitigate espionage, these data centres may still be susceptible to sabotage or cyber incidents. Sabotage of undersea communications as a physical security issue, does present a further risk to the stability of the Internet and online services.

Undersea oil and gas pipelines may also be targeted by state actors and cybercrime groups. The Colonial Pipelines incident demonstrated the potential disruption that ransomware can cause, including panic buying. It is therefore feasible that a similar incident with a major undersea pipeline supplying a large percentage of national oil or gas can cause severe national shortages of the commodity and result in a nationwide panic buying. With the alleged physical sabotage of undersea pipelines in the Baltic Sea, cyber operations may be an alternative avenue to sabotage the pipelines.

Maritime Cybersecurity: Perspectives from Critical Infrastructure Protection and Economic Information Warfare

Critical infrastructures often have an interdependence, and the maritime domain is inter-related to several other sectors. The objective of the domain is primarily transportation (of freight or people), and the maritime domain is one section of a longer supply chain, including roads, rail, and pipelines. However, a large proportion of trade moves through the ports which connect to multiple land transportation routes. The ports can be considered as 'critical nodes' within a broader interconnection of transportation routes; should a disruption at a major port occur, this causes backlogs on the rails and roads; alternatively, disruption of the rail and road infrastructure could result in import freight clogging the port while export freight cannot reach the port.

A challenge for cybersecurity in the maritime domain of ports is that there may be a *mix of legacy systems* (particularly for operational technology) *as well as modern technological innovations*, such as the industrial internet of things (IIoT) and remote network management. Legacy systems and operational technology could rely on outdated operating systems for which there are no longer any security updates, leaving vulnerabilities in the infrastructure. Modern technologies are sometimes not designed with security as a key consideration, which also introduces vulnerabilities.

Associated with this is the concept of *economic information warfare*, where a hostile nation or group could target facilities for economic espionage purposes, or cause disruptions to negatively impact a victim nation's trade and economy. With large quantities of freight transiting through ports, cyber incidents targeting specific terminals can disrupt particular commodities to impact on national economies and international commodity prices. Similarly, the landing points for undersea cables are a convenient facility to conduct espionage due to the information flow through that specific point. Disrupting the landing points, thereby reducing the international information flow, could impact on a nation's international trade due to degrade information exchange.

Stemming from the incidents described above, hypothetical incidents to disrupt activity in the maritime domain can be considered, such as: (1) spoofing GPS so automated equipment navigate into the water; (2) spoofing GPS so a ship runs aground in narrow channels; (3) malware interfering with the ballast tanks of a submersible; (4) automated mooring systems in heavy weather so ships break their moorings; (5) erratic behaviour is induced in cranes or conveyer belts to force a shutdown; (6) using a time-activated logic bomb aboard a vessel to infect USB drives copying information to the port systems; (7) compromising fleet management systems to deliver malware to vessels; (8) affecting valves to fluctuate the pressure in undersea pipelines.

Best Practices, Policy and Regulation

It is important for all organisations operating in the maritime domain and transportation infrastructure to identify key facilities and systems. Single points of failure need to be identified – this can range from a key port or a single network switch which the enterprise IT infrastructure relies upon. This can be achieved through cybersecurity risk assessments, which will aid in identifying and prioritising important systems for the implementation of cybersecurity controls (preventative and detective). An economic analysis of ports and associated pipelines and rail routes can assist in determining the potential economic impact of a cyber incident. Cybersecurity risk assessments should not be limited to the corporate IT infrastructure but needs to extend to all systems that have presence on any network (even if it is air gapped). The BIMCO *et al.* (2021) guidelines provide examples of risk assessments for systems aboard ships. In addition, identifying threats and engaging with threat intelligence platforms can be beneficial.

It is important that operational technology, IIoT and legacy systems, should be segregated from the corporate network using air gaps, firewalls, or virtual LANs (VLANs). Should remote connectivity be required for these devices, then this should be strictly controlled and facilitated in such a way that there is no direct connection to the Internet. Similarly, the core network of undersea cables needs to be segregated and any remote network management tools needs to be strictly controlled. Strong authentication/access control and communication security mechanisms should be employed and regularly reviewed, and any privileges or connections that are no longer required should be removed. Service level agreements with vendors and service providers should clearly state security requirements and expectations, as the security components are often ambiguous or incorrectly assumed to be included in the services.

An important concept is *security by design*: involving cybersecurity experts in the design and implementation of new systems from the beginning of the project to minimise vulnerabilities. It is easier and cheaper to implement security within the design than attempting to implement security retrospectively. Cybersecurity response plans need to be in place to guide how individuals respond to possible incidents. For example, a challenge is to have cybersecurity incident response on seagoing vessels in the event of catastrophic system failure due to malware and incorrect procedures may result in the situation being inadvertently escalated rather than contained. The incident response plans should include corporate communications, legal services, and other functions for a holistic approach.

In addition, *cybersecurity awareness* of all employees, including bridge crew and those operating key connected systems aboard vessels and in ports, is important so that they can respond appropriately and report suspicious behaviour (such as scam emails or erratic system behaviour) that could indicate there is a cyber incident underway. As part of the awareness training, personnel who will be expected to assist with cyber incident response and recovery procedures can wargame the processes to ensure they are familiar with the incident response plan.

Relevant regulation, policy and guideline documents that can be considered to further support cybersecurity in the maritime domain are:

- Maritime-specific documents
    - International Association of Ports and Harbors (IAPH) *et al*. Port Community Cyber Security
    - ENISA Report on Port Cybersecurity
    - IMO Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems
    - IMO MSC-FAL.1/Circ.3/Rev.1 (2021) Guidelines on Maritime Cyber Risk Management
    - BIMCO et al. The Guidelines on Cyber Security Onboard Ships
    - ENISA Report on cables
- Other cybersecurity documents
    - ISO/IEC 27001 Information security management systems
    - ISO/IEC 27032 Cybersecurity
    - National Institute for Standards and Technology (NIST) Cyber Security Framework
    - ISA/IEC 62443 standards for industrial automation and control systems
    - MITRE ATT&CK Framework for industrial control systems

Legal documents may be more difficult to interpret; while this is outside the scope of this briefing, for completeness some considerations are as follows. National legislation will be applicable for ports, cable landing stations, and matters within territorial waters, and will need to be interpreted for their relevance to cyberspace. For international waters, the UN Convention on the Law of the Sea (UNCLOS) applies, and Chapter 8 of the Tallinn Manual 2.0 on the International Law applicable to Cyber Operations discusses the UNCLOS in terms of cyber operations.

Conclusion

Cyber incidents have affected ports and vessels, and to a lesser degree undersea infrastructure. These incidents demonstrate that operations can be affected by malware (including ransomware) and other malicious activities; it is therefore viable for targeted cyber operations by a nation state to disrupt specific commodities or the national economy of the victim nation, or cyber criminals to exploit the criticality of the infrastructure to extort large payouts and inadvertently have large economic impacts.

Several hypothetical incidents are proposed for consideration in conducting security risk assessments. Best practices include common cybersecurity control implementations; however, risk assessments of key operational systems need to be implemented.

Recommended for further reading.

Pretorius, B.H. and van Niekerk, B. (2020). Industrial Internet of Things Security for the Transportation Infrastructure, *Journal of Information Warfare* 19(3), pp. 50-67.

van Niekerk, B. (2017). Analysis of cyber-attacks against the transportation sector. In: M.E. Korstanje (ed.), Threat mitigation and detection of cyber warfare and terrorism activities, Hershey, PA: IGI-Global, pp. 68-91.

van Niekerk, B. and Ramluckan, T. (2019). Economic Information Warfare: Feasibility and Legal Considerations for Cyber-Operations Targeting Commodity Value Chains, *Journal of Information Warfare* 18(2), pp. 31-48.

Prof Brett van Niekerk is from Durban University of Technology and a Research Fellow with SIGLA.

Email: BrettV@dut.ac.za

GUEST LECTURE BY AUTHOR

Please scan for more information on the related hybrid guest lecture on 27 September 2023 at the Faculty of Military Science.

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

16 PEACE, JUSTICE AND STRONG INSTITUTIONS