Canadian Coast Guard | Garde côtière canadienne

INDUSTRY DAY:
MARITIME CYBERSECURITY FROM SHIP-TO-SHORE

RESULTS AND PATH FORWARD REPORT

Canada

Industry Day : Maritime cybersecurity from ship-to-shore - Results and path forward Report

Published under the authority of:

Fisheries and Oceans Canada
Canadian Coast Guard
Ottawa, Ontario K1A 0E6

Cat. No. Fs23-707/2023E-PDF
ISBN: 978-0-660-48380-1

2023-04-18

Available on the CCG internet site

Disponible en français :
La journée de l'industrie : Cybersécurité maritime du navire à la côte - Rapport sur les résultats et la voie à suivre

Cat. No. Fs23-707/2023F-PDF
ISBN : 978-0-660-48381-8

Table of content

Executive summary

The Canadian Coast Guard (Coast Guard) hosted an event “Industry Day on Maritime Cybersecurity: From Ship-to-Shore” bringing together stakeholders from industry, government, and academia to discuss maritime cyber risk and to assess options for ensuring cyber resiliency in the maritime sector. This full day event, held on February 2nd, 2022, saw significant attendance with almost 300 virtual participants, helping to generate awareness on the latest cybersecurity threats in the maritime sector.

The event included presentations from federal departments, Canadian shippers, port authorities, maritime cybersecurity companies, vessel classification societies, domestic and international maritime first responders, cyber experts, and regulators. This sharing of information, from a diverse set of maritime stakeholders, allowed for an improved awareness of the threat actors and their impacts and for the exchange of best practices on how to ensure the resiliency of this critical sector despite an unseen level of connectivity between information technology (IT) and operational technology (OT) systems.

Key topics discussed were how to increase the cyber resiliency of the maritime sector (e.g., cybersecurity of vessels, ports and cargo terminals), the need for increased maritime cybersecurity training, funding for medium to smaller ports, creating and maintaining a robust cybersecurity workforce for digital seafarers, and increasing cyber risk information sharing.

This Results and Path Forward report has recommendations for collaboration on sector specific maritime cybersecurity training, maritime cybersecurity funding, cybersecurity information sharing, maritime cybersecurity supply chains, and maritime cybersecurity authorities.

Introduction

Canada is a maritime nation, and the maritime industry has been crucial to the development of Canada. The maritime industry has influenced national economic development, the location and growth of cities, and the livelihoods of Canadians for generations. The maritime shipping industry contributes three billion dollars a year to Canada's GDP and falls under the critical transportation infrastructure sector. Indirectly the maritime industry contributes to the employment of over 100,000 Canadians and generates $4.6 billion in labour income.[1] Maritime trade enables global and regional supply chains which supports the functioning of Canadian lives on a daily basis.

In 2017, recognizing the exponential increase in cyber attacks on the maritime sector, the International Maritime Organization (IMO), a specialized agency under the auspices of the United Nations, issued a resolution making it mandatory for SOLAS (Safety of Life at Sea) Class vessels to implement cyber risk measures into their organization’s safety management systems by January 1, 2021. Maritime cyber attacks have impacted not only vessels and their functionality, but also ports and terminal operators, affecting operations and causing hundreds of millions in damages due to data loss and cargo backlogs.

According to one maritime cybersecurity company, the average payout to cyber criminals for an attack in the maritime sector is estimated to be USD $3.1 million.[2] Moreover, state actors and their proxies are actively targeting the navigation, communications, and industrial control systems of vessels, ports, and cargo terminals to inflict maximum damage.

Unsecure and unsegmented systems have the potential to cause marine equipment to become inoperable, leading to a host of significant impacts in this critical sector. The Coast Guard itself is not immune when threat actors make attempts on critical systems, including the marine communication systems. If those systems were disrupted during a search and rescue emergency response, distress messages might not be received. Therefore, it is crucial that government continues to build common maritime cyber security information sharing approaches with allied nations and industry.

Mitigating cyber risk requires not only an understanding of the convergence between OT and IT systems, but also how these systems vary compared to generic IT. For instance, while employees with ship and shore-based jobs will both have email and Wi-Fi just like office jobs, what makes the sector unique is the navigation systems (Electronic Charting and Display and

Information Systems, GNSS, radar), the industrial control systems (ICS) (e.g. cargo handling, human-machine interface, propulsion/steering, OT, the communications systems (AIS, satellite link, VoIP), as well as loading and stability systems (e.g. hull / ballast systems, water filtration). Similarly, shore-based jobs at ports have a parallel issue with the complexity of their systems, gantry controls, SCADA, PLC systems, as well as communication and IT servers which are offsite. Likewise, cargo traversing waters also rely on many ICS and IT systems, such as shipper data centres, IT infrastructure or OT systems that influence tank monitoring systems for oil and natural gas to be safely transported and stored. The intersection between critical safety requirements and remote monitoring capabilities makes monitoring these systems a potential cyber incident waiting to happen, unless the systems are properly secured and segmented.

The variety and complexity of these systems and the speed in which they connect with the internet has not kept pace with security measures to protect them from nefarious threat actors. Coast Guard plays a key role as an enabler in this critical infrastructure sector, preventing flooding through icebreaking or clearing shipping lanes of ice to ensure economic prosperity; pollution response; emergency response and search and rescue; support to law enforcement; and ensuring Canada’s sovereignty in Arctic waters. Further to Coast Guard’s traditional services, Coast Guard is using an all-hazards approach to ensure the risk based response to maritime cybersecurity is proactive not reactive.

The state of maritime cybersecurity

The security landscape has evolved over the past 20 years from focusing on physical security to having to manage cyber threats originating from increased interconnectivity. Government and industry response has not been able to keep pace with the interconnectedness between OT and IT. In 2019, a survey found that 68% of manufacturers plan to increase their investment in IT-OT convergence over the next two years. In 2020, there were well over 500 severe OT system cyber attacks that hit the maritime industry. This is significant, as ports and vessels are predicated on a combination of IT and OT systems reflecting an increased cyber vulnerability within the maritime sector.

While increased efficiencies may help the sector obtain their financial goals, unsecure software or unsegmented marine equipment may have cascading effects if cyber-risk is not appropriately addressed. Since the onset of the pandemic in 2020, one cybersecurity company has noted a 400% increase in attempted hackings of the maritime industry's IT and OT systems, whereas there has been a 900% increase in cyber attacks targeting OT located at ports and on vessels.[3] In 2021, the *Ever Given* mega-container ship blocked the Suez Canal for six days. By blocking the canal, it cost the global economy $400 million dollars USD per hour with an estimated total trade loss of roughly $54 billion USD. While the cause of this incident was high winds, a cyber attack can certainly result in a vessel running aground or capsizing. These examples demonstrate how very real the threat of maritime cyber risk is to the safety and economic prosperity of vessels in Canadian waters.

At port terminals cyber attacks on ICS, can be extremely disruptive. For instance, most of the cranes at smart ports are constructed and operated by one company overseas and run on 5G networks and other automated services. If that company were affected by a cyber attack or compelled by a state-owned entity to stop those cranes from functioning, then they would effectively shut down operations, causing ports to come to a standstill in a matter of seconds across Canada.[4] One research firm revealed a similar operation in 2019 by controlling several large cranes.

According to open sources, there are strong indications that hostile state actors are remotely targeting vessel ICS and supervisory control and data acquisition (SCADA) systems, such as ballast water and filtration, with the intention of sinking vessels and causing irreparable damage and causalities. Nation states hold a repository of vulnerabilities on maritime equipment to

leverage them for maximum effect during war time or increased sanctions.[5] This is occurring as hostile states are increasing their offensive cyber capabilities.

Maritime cybersecurity supply chains are also the prime targets of cyber attacks. In 2019 state-sponsored activities by advanced persistent threats (APT) targeted universities in Canada to acquire maritime and naval technology. This information is extremely valuable to adversarial nations, as it can give them leverage over a foreign Navy or Coast Guard and their intellectual priorities. Once inside supply-chains, threat actors may seek to disrupt the critical operations of vessels and critical maritime communication services.

Hostile states are actively seeking to exploit maritime communications equipment for internet-exposed devices which are used globally to reveal log-in screens from internet searches. These actors are leveraging websites such as *Shodan* to show how devices and information systems are connected to the internet and how they can be remotely monitored and controlled. This raises questions of internet connected devices, the integrity of marine equipment and original equipment manufacturers (OEMs) to ensure the confidentiality, integrity, and accessibility as well as *quality* materials used to manufacture that equipment.[6]

There are numerous examples in which a cyber attack on IT systems has led to OT impacts. For example, in 2019, the United States Coast Guard responded to a disabled, infected vessel that had unsecure, unsegmented systems in the Port of New York and New Jersey. The vessel reportedly had ransomware burrowed into the OT of the vessel, rendering the vessel inoperable.

According to some industry specialists who surveyed the maritime industry in 2021, of those who experienced cyber attacks, 40% experienced significant or severe cyber attacks, while 52% experienced minor incidents. In terms of cybersecurity training, only 26% of those polled felt that enough is being done to spread awareness of cybersecurity. Additionally, only half of respondents said they were offered some form of cybersecurity training. Including training on cyber hygiene, as it relates to IT and OT systems, would help to mitigate human risk in the maritime sector.

New research by a maritime cybersecurity company in 2022 found that when cyber attacks in the maritime sector led to ransom payment, ship owners paid on average more than $3.1 million USD to cyber criminals. Research also found that shipowners significantly under-invest in cybersecurity management with the majority of ship owners spending less than $100,000 USD per year on cybersecurity. This lack of investment could be a result of companies being lulled

into a false sense of security due to endemic under-reporting of the actual number of cyber attacks.

Many maritime organizations have yet to realize the risk to systems and the range of threats facing this sector. In 2017, the IMO adopted Resolution MSC.428(98) *Maritime Cyber Risk Management in Safety Management Systems,* a resolution requiring ship owners and operators to implement cybersecurity considerations into their safety management systems by January 1st, 2021. While these types of international resolutions are important and have led many international associations to set guidelines and requirements, there is a lack of governance structure which has been criticized for not being able to progress other issues such as interconnectedness.

Coast Guard is a critical infrastructure owner and operator responsible for its assets and services from clearing shipping lanes of ice for commerce, icebreaking to prevent flooding, support to law enforcement, emergency response, and search and rescue, ensuring sovereignty in Canadian waters, pollution response, marine traffic and communication services as well as aids to navigation. It is the primary responsibility of owners and operators of critical infrastructure to strengthen their resiliency to deal with foreseeable disruptions and disasters. Due to exponential levels of connectivity and the convergence of IT and OT systems, the maritime sector must collectively be prepared for the inevitable.

Through its role as the co-chair for the CAN-US MDA partnership: Cyber assessment working group, the Coast Guard continues to draw attention to the interconnectedness of the maritime sector and its vulnerabilities. In addition, by leading the International Association of Marine Aids to Navigation Cybersecurity Workshop (2021) and chairing the newly created Five Eyes (FVEY) MDA Partnership Cyber Working Group (2022), Coast Guard continues to advance its knowledge regarding the threat landscape from a seafarer’s perspective and how to mitigate worst-case scenarios. This requires recognizing that all maritime stakeholders play a part in this critical transportation infrastructure sector. By bringing industry and government together to expose common threats and aligning efforts, only then can true progress be made.

Industry day: summary of panel and thematic discussions

Overview of panel 1: maritime cybersecurity certification and class notation

This panel surveyed what some industry specialists are doing to empower workforces with skills and tools to understand the maritime cybersecurity threat landscape.

Opening remarks by Canadian Coast Guard's Director General of Fleet and Maritime Services. The panel was moderated by Canadian Coast Guard with panelists from Bureau Veritas, Neptune Cyber, Nettitude (an LRQA company).

Summary

- As the lines are blurred between IT and OT systems, worst case scenarios are now becoming the reality given the level of interconnectedness from ship to shore.
- Maritime cybersecurity training is the most impactful action organizations can do; it is a responsibility not just for IT experts, but the entire workforce.
- Spectrum disruptions via spoofing or jamming cause significant navigational hazards by manipulating critical infrastructure systems such as automatic identification systems (AIS).

Thematic discussion

The number of cyber attacks is breaking records every month. In 2021 cybersecurity attacks costed an estimated $6 trillion USD globally. By 2025, it will likely reach $10.5 trillion USD. Nation-states and cyber criminals are conducting operations and are watching maritime organizations every day. Threat actors get through these exposed surfaces either through the vessel or business enterprise. A means of compromising a vessel could be another way of compromising all vessels in the fleet.

Nightmare scenarios, such as fleet blackouts, are today's reality as hackers broaden attack spheres and find new ways to compromise systems. The boundary between IT and OT is harder to define resulting in a vulnerability which can be exploited on hundreds of ships. Threat actors may prey on a lack of digital culture in an organization and once inside a ship's network systems it is unclear what level of difficulty they would face before being able to remotely manipulate the ship's steering, ballast pumps and navigation. The maritime sector is faced with

fundamentally different issues than office cybersecurity. Ships are now interconnected in ways that pose a problem for those who are not trained in maritime cybersecurity. Vessel owners and operators must be able to identify IT/OT assets and the way they are interconnected or connected to shore.

For instance, a ship's internal network interconnects with various systems required to keep the vessel afloat, as well as an external network to keep it operating efficiently. The International Association of Classification Societies (IACS) recognizes the risk that unsecure and unsegmented vessels pose. To mitigate this risk, in 2022, IACS adopted two new Unified Requirements (URs) providing minimum goal-based requirements for the cyber resilience of new ships and for the cyber security of onboard systems and equipment. These URs will be applied to new ships contracted for construction on and after 1 January 2024.[7] That means cybersecurity considerations must be applied throughout the lifecycle of the vessel, from the design phase through to the construction, operational, maintenance and decommissioning phases. Additionally, some major shipyards are currently implementing this requirement this year with the assistance of class societies and maritime cybersecurity companies.

One of the single biggest, and most impactful actions the maritime sector can take is training on maritime cybersecurity. This training should be focussed on the entire workforce and not just IT experts. The IMO has an expectation that each organization has effective measures through its safety management system to handle cyber risk. Mitigation includes having crew members who have special responsibilities for handling cybersecurity on board. For instance, having a ship master or chief IT officer aboard with the responsibility to update computer systems, apply the latest software patches, as well as keep charts and other navigation systems updated. For many workers with shore-based jobs working with generic IT systems, this means adhering to basic principles of cyber hygiene. For ship owners and operators there is increasingly an expectation of cyber literacy. It only takes one untrained employee to unknowingly spread ransomware throughout an enterprise system, costing millions in damages, or rendering its operations inoperable.

Spoofing AIS is another example of an attack that is relatively easy for threat actors to employ; however, innovative solutions will be required to provide sufficient defence against such attacks. Maritime cybersecurity companies are working with academia, such as Polytechnique Montreal, to come up with innovative solutions to detect and stop these types of cyber attacks from occurring.

Overview of panel 2: Maritime cybersecurity guidance and cyber supply chain risk management

This panel delved into what maritime cybersecurity guidelines are being recommended for ship owners, operators, and ports both nationally and internationally. Additionally, it explored various risks in maritime cybersecurity supply chains.

The panel was moderated by Bastionnage Consulting Inc with panelists from Transport Canada (TC), Public Service and Procurement Canada, and the United States Coast Guard.

Summary

- Maritime cyber supply chains are threatened not only by counterfeit materials, but also through IT system backdoors being exploited by the sophisticated methods of state actors and their proxies.
- The Cybersecurity Maturity Model Certification (CMMC) builds consumer confidence in an organization's ability to produce security by design products and services.
- The United States Coast Guard is increasing the capacity of its cyber workforce to detect and defend against those who seek to disrupt the maritime sector.

Thematic discussion

In terms of gaining access in the supply chain from a cyber perspective, there was a recent attack where a technology firm was subject to a cyber attack that spread to its clients and went undetected for months. This hack involved malware creating a backdoor to customers IT systems installing malware that led to the theft of intellectual property and sensitive information. Defence and maritime sector supply chains are prime targets for cyber attacks. In 2019 there were state-sponsored events targeting universities in Canada to acquire maritime technology.

The US Department of Defense is leading in terms of adopting cyber certification from vendors and suppliers in their supply chain, such as new regulations requiring all contractors within their supply chain to be accredited according to CMMC standards. The Government of Canada is assessing options on how to address supply chain cybersecurity requirements in the context of CMMC. Many organizations, such as the US Department of Defense take security by design seriously and only procure marine equipment from vendors and suppliers who are certified using the CMMC.

The need for cybersecurity supply chain certification was put forward. This promotes smart consumerism: security by design throughout the life cycles of ports, vessels and cargo terminals. This is important since IT system backdoors and lack of awareness of cyber risk may result in relaxed standards when procuring electronic materials. Given the interconnected nature of marine IT, OT, and PNT systems, vulnerabilities in supply chains can have catastrophic domino effects. Thus, insecurity in the supply chain of one vendor can affect the products of other vendors once integrated on the ship or port side. There are physical controls to protect life and property such as escorts through water borne assets when a vessel may be compromised.

The USCG in response to 9/11, built a Cybersecurity framework that requires maritime operators to assess their systems, networks, and facilities for vulnerabilities and to formulate a security plan to address these gaps. Through interagency collaboration, the USCG has been building resiliency into networks, with the aim of mitigating incidents before they occur.

USCG cyber role aims to have it as a recognized leader in maritime safety and security, building strong public-private partnerships to engage with stakeholders, improve cyber awareness, and enhance information sharing processes. Outreach includes cyber threats, risks, vulnerabilities, and best practices as well as engagement in cyber workshops, conferences, and public outreach. USCG issues guidance for industry and stakeholders via cybersecurity framework profiles, navigation, and vessel inspection circular (NVIC) 01-20, work instruction on vessel cyber risk management, as well as their in-progress Maritime Cyber Risk Assessment Model. Additionally, USCG has employed Marine safety and Cybersecurity advisors to help educate the maritime workforce and includes cyber hygiene in routine general marine inspections.

Overview of panel 3: Cyber-physical safety, and industrial control systems

This panel examined cyber physical safety in ICS as well as what cybersecurity services and training are available to the maritime sector. Additionally, it explored working together on increased information exchange and towards establishing a community of practice on maritime cybersecurity.

Panel three was moderated by Bastionnage Consulting Inc and featured panelists from Association of Canadian Port Authorities, Canada Steamship Lines Groupe Inc, Public Safety Canada (PSC), and the Canadian Centre for Cybersecurity (CCCS).

Summary

- The Canadian Government is continuing to advance policies on maritime cybersecurity in terms of standards, information sharing, coordination and decision making.
- Ports, vessels, and cargo terminals are being exposed to additional vulnerabilities due to their ongoing reliance on IT, OT and PNT systems.
- Increased investment in training is required in order to prepare the next generation of cybersecurity specialists.

Thematic discussion

Ports, vessel operators, and maritime cybersecurity companies have expressed a desire to receive more cyber risk information given its impact on business operations. Moreover, Canadian shippers and the Association of Canadian Port Authorities have expressed that they would see added benefit from a regular forum on information sharing further to the current event.

The panel made it evident, that there needs to be enhanced awareness of the convergence of IT and OT and how critical infrastructure and emergency management needs to work together to establish decision making processes.

It is often unclear where to find effective training and awareness on OT specific to the sector. Investment in cybersecurity training is currently in short supply. A small number of universities and colleges, such as Polytechnique Montreal, work on domain specific maritime cybersecurity. While several educational institutions provide cybersecurity training related to critical

infrastructure, few are specific to the maritime sector. Canadian maritime shippers have noted that there is a direct correlation between investments made in training cybersecurity students and the industries they enter. The US, UK and Israel have already made these investments in sectors specific expertise.

In Canada, port authorities are vigilant, and many have developed their own capacities in terms of cyber response; however, a majority of the 550 medium to small sized ports do not have the resources the larger ports have, and therefore lack cybersecurity response capacity. The ACPA state that a cyber attack could have regional supply chain domino impacts to the smaller ports depending on the type of incident. It is necessary to have an appropriate cyber framework in this sector, as well as the capacity to respond effectively to loss of life, pollution, or barriers to shipping lanes (e.g., grounded ship) due to a cyber incident.

Cargo terminal operators and shipping agents tend to control the IT and OT systems related to the movement of goods. The level of interconnectivity has created additional exposures that has resulted in shipping agents and cargo operators being targeted during social engineering schemes. This has caused many terminal operators to be seen as the epicentre for cybersecurity attacks at many ports around the globe and in Canada.[8] Cyber attacks on cargo terminals are very noticeable as they will create an additional backlog of loading and unloading with operations grinding to a halt.

In terms of vessel operators, Canadian shippers have signaled their desire for government incentives to increase cybersecurity in the maritime sector. Incentives can be created to push companies to conduct phishing tests, carry out employee training, have better cyber insurance, migrate data to the cloud, adopt standards such as CMMC and become accredited. Cyber experts in the CCCS offer no-cost services, cybersecurity information alerts and bi-weekly calls with the transportation sector at large. Moreover, Public Safety Canada helps critical infrastructure owners increase their resiliency through their symposiums, workshops and tabletop exercises.

Additionally, as pointed out by academics during the discussions, much of the current debate focuses too much on the short term: ransomware and generic cybersecurity problems for which there are solutions, and it does not focus on those *black swan* events that deal with IT, OT and operations.[9] Academics have noted that government needs to start looking at worst-case scenarios, so that owners and operators can start building a forward looking roadmap. Solutions must keep pace with evolving threats and hazards.

Planning and simulating future cyber challenges through tabletop exercises between industry and government prepares the maritime sector for an inevitable cyber-attack and secondary hazards such as search and rescue, pollution response and boarding. These tabletop exercises inform the creation of a possible maritime cyber risk frameworks and threat matrixes desired by Canadian Port Authorities (CPAs), and maritime cyber experts. Additionally, tabletop exercises have the benefit of helping the maritime sector understand their risk exposure.

Issues and recommendations

The following issues and recommendations are based on observations and the collaborative discussion that took place during the Industry Day event. As a result, they are presented with non-attribution to any stakeholder attending the event.

Maritime cybersecurity training

There is a necessity to bridge the gap between information experts, operational experts, and maritime sector operators. In other words, these three communities do not speak the same language, nor do they have the same priorities. There is a significant need to begin training the workforce of the future to deal with problems of the future. This process must begin as soon as possible as it often takes five to six years to fully train sector specific personnel. Therefore, the necessity of building a new generation of experts who are cognisant of all three aspects: cyber, ICS, and operations is imperative. It is necessary that maritime sector stakeholders remain forward thinking in relation to future problems. Another vector of attack are the trusted agents who enter ports, many businesses, contractors and visitors may not have the same level of cybersecurity training (such as cyber hygiene) as port personnel. A tabletop exercise may help prepare for future simulated conditions and help resilience.

Recommendations

- Continue to work interdepartmentally and internationally to assess educational models that are recognized by the IMO and international class societies. This also contributes to ensuring the basic mandatory level of security training standards for crews interacting with OT and IT systems are developed.
- Continue interdepartmental discussions to explore cyber security work placement opportunities, within the federal government, focussed on the maritime sector.
- Engage interdepartmentally to continue to ensure the maritime sector is appropriately referenced in the Cybersecurity Action Plan.
- Vessel owners, ports and cargo terminal operators are encouraged to work with maritime cybersecurity companies and/or class societies to increase their cybersecurity profiles in terms of security controls being applied and systems within their scope and explore workshops and training offered by PSC and the CCCS.

- Engage interdepartmentally, and potentially with Industry, to plan or leverage an existing tabletop exercise to simulate a potential cyber threat in a maritime environment.

Maritime cybersecurity funding

Any form of raising levels of cybersecurity for non-port authorities will require significant investment in terms of monetary resources and human resources from the government to achieve. Currently there are 19 remote ports under TC‘s ownership, and they own some of the 31 regional ports out of the 550 public ports. There is a need to update aging and outdated port infrastructure, and stakeholders are looking to ask the federal government to create cybersecurity policy not only for Port Authorities but also small to medium sized ports.

To highlight the interconnected nature, a 2019 simulated case study by the *Cambridge Centre for Risk Studies* explored the potential impact of a computer virus transmitted by ships to connected ports. In one worst case scenario, the virus destroyed the cargo database at 15 ports in Asia and caused as much as $110 billion in damages, $101 billion of which would be uninsured.[10] This case study highlights the vulnerabilities of aging critical port infrastructure during an area of high-paced interconnectivity. If a nefarious actor cannot gain access to the port’s server, they will try to compromise a tenant that has trusted access to the port’s network.

Recommendations

- Continue to work to identify new and existing funding opportunities in the maritime cyber domain including public-private initiatives.

Mitigating positioning, navigation and timing disruptions

Jamming devices (interference generators or signal suppressors) are prohibited in Canada. Issues related to positioning, navigation and timing (PNT) systems disruptions have an immense potential impact on the maritime sector, particularly when it comes to shipping operations. Global positioning system (GPS) and automatic identification system (AIS) jamming and spoofing problems have been well documented for many years, and issues related to signal loss are magnified in the confined space of a port. According to academics in the Atlantic Council “AIS is among the most critical systems in the maritime industry as it allows for the exchange of vessel positioning and information alerts... the potential effects of compromised [positioning, navigation and timing] are significant, as modern ships rely heavily on these

satellite and radio based systems for navigation."[11] Attacks on navigation system can be individually disruptive by delaying the arrival at port of a single ship or they can be globally disruptive by causing a vessel to run aground, blocking a port or waterway for days or longer.

Coast Guard is the key owner and operator of AIS and other maritime critical infrastructure in Canada. One of the most significant cyber threats are the threats to AIS, and other navigation systems. GPS spoofing has become so common in some parts of the world that many consider the system unreliable and frequently resort to navigation by other means.

Recommendations

- Explore options (authorities, technologies) to detect, combat, and mitigate the effects of AIS and GPS jamming and spoofing in Canada's waterways.[12]

Information sharing

Maritime cyber risk information is a critical information requirement, which directly supports well-reasoned and timely decision-making. This points to the importance of timely sharing and protection of information among partners. However, reporting on cyber incidents as they relate to ports and vessels is not a requirement in Canada (except on matters related to breaches as per the Personal Information Protection and Electronic Documents Act). In fact, many maritime sectors businesses fear that if they report their information, it can hurt their reputation. Sharing cyber-risk incident information can aid in determining actual risk in this sector especially if the organizations receiving incident information have a strong disclosure program guaranteeing anonymity, such as the reporting mechanism at CCCS.

Recommendations

- Coast Guard will continue to hosting an annual *Industry Day on Maritime Cybersecurity* to promote cyber security resiliency and increased information exchange between government and industry partners.
- Investigate how best to build a relationship with the US Maritime Transportation System Information Sharing Analysis Centre (MTS-ISAC) noting the subscription based model of participation. The MTS-ISAC offers an Information Sharing Service for maritime critical infrastructure stakeholders, serving as a centralized point of coordination to share timely and actionable cyber threat information between trusted stakeholders.
- Continue to foster a level of trust with industry and academia to facilitate the sharing of best practices and advance the discussions around maritime sector cybersecurity to enable the development of joint cyber solutions.
- Explore methods for enhancing the dissemination of cyber risk information to maritime stakeholders during emergency and non-emergency situations.

Maritime cybersecurity in supply chains

The maritime sector is an interconnected industry that requires a holistic understanding of the needs of key stakeholders and the risks they can expect as non cyber experts. However, inaction serves threat actors into exploiting vulnerabilities. A cybersecurity company conducted a survey of the maritime sector this survey sample included seafarers, shoreside managers, and suppliers. They found that only 55% of industry suppliers are asked by ship owners to prove they have cyber risk management procedures in place. When commissioning marine equipment by default it is easy to access by the procuring organization. In some cases, manufacturers may bring the equipment to an appropriate security level for the organization to meet their needs. However, not all organizations do this, and this easily accessible equipment introduces cybersecurity vulnerabilities. It is best that original equipment manufacturers (OEMs) create products with security by design, which may require standardizing a product and penetration testing through firmware.

Recommendations

- If possible, it is recommended to purchase electronic equipment and software from vendors that have adopted, or in the process of adopting, *NIST 800-161 Supply Chain Risk Management, ISA99 Standard on Developing Products that are Cybersecure by Design, and ISO 28000s*. If possible, procure equipment from vendors or suppliers that have adopted or are engaged with CMMC accreditation.
- Support the International Maritime Organization when they consider the development of secure-by-design guidelines.

Maritime cybersecurity authorities

When a virus is transmitted by a port tenant which disrupts operations, port tenants affect the overall operations of Port Authorities, causing backlogs to the loading and unloading of cargo and possibly resulting in vessel jams. The Association of Canada's Port Authorities requested more clarity around the coordination and decision-making processes and authorities of federal departments and agencies. This stems from the many threat surfaces specific to the maritime domain, including ports, ships, maritime traffic control centres, unmanned autonomous vessels and their individual systems IT and OT systems.

Canada is a signatory state to the IMO, a United Nations specialized agency responsible for measures to improve the safety and security of international shipping and to prevent pollution from ships. As per the IMO guidance on Maritime Cyber Risk Management, ports should also take an all-hazards approach to maritime cybersecurity by implementing cyber risk into their business continuity plans. An all-hazards approach is necessary in this critical transportation infrastructure sector in order to build the capacity to respond to threats and keep hazards from becoming disasters.

Recommendations

- As a community there is a need to continue to develop a way forward on this aspect of the conversation, including further discussions at upcoming 2023 Industry Day event.

Conclusion

The engagement in this sector has been both meaningful and valuable in terms of raising the waters on maritime cybersecurity awareness and information sharing. It also shows what is at stake in order to protect the maritime sector as one of the key critical infrastructure sectors. Federal partners and industry have a shared responsibility to identify and manage maritime cyber risks and will continue to work together to align approaches on maritime cybersecurity to ensure cyber resiliency from ship-to-shore.

Cyber is woven into everything government and industry does, and the Industry Day on Maritime Cybersecurity aligns with and compliments many other documents such as the *National Cybersecurity Strategy*, and the *National Strategy for Critical Infrastructure*. As Coast Guard and others test maritime autonomous systems, we must be cognisant that we are grasping a double-edged sword, full of opportunities as well as attack vectors that could be leveraged by malicious cyber actors in an era of increased connectivity.

Coast Guard and the broader maritime sector must be involved in continuous learning in the maritime sector. Given this, government is engaging with industry to collectively protect the maritime sector and raise awareness of maritime cyber risks. The end is to support a safe and secure shipping sector which is operationally resilient to cyber risks. Coast Guard looks forward to working with industry, academia, and other government departments to continue to advance solutions on how to best protect the maritime sector.

Annex I: Glossary

Automatic Identification System (AIS) is an automatic tracking system that uses transceivers on ships and is used by vessel traffic services (VTS) to ensure collision avoidance on the water.

Advance Persistent Threats is an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing/extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future.[13]

Backdoor is an undocumented, private, or less-detectable way of gaining remote access to a computer, bypassing authentication measures, and obtaining access to plaintext.

Critical infrastructure refers to the processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. There are ten critical infrastructure sectors: Energy and utilities; Finance; Food; Transportation; Government; Information and communication technology; Health; Water; Safety; and Manufacturing.

Cyber attack is the use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device

Cyber incident is any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable any computer network or system resource.

Cybersecurity The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cybersecurity includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.

Cyber threat A threat actor, using the internet, who takes advantage of a known vulnerability in a product for the purposes of exploiting a network and the information the network carries.

Information Sharing and Analysis Centers (ISACs) are non-profit organizations that provide a central resource for gathering information on cyber threats, in many cases to critical infrastructure, as well as allow two-way sharing of information between the private and the public sector about root causes, incidents and threats, as well as sharing experience, knowledge and analysis.[14]

Information technology (IT) systems refers to the application of network, storage, and computer resources toward the generation, management, storage, and delivery of data throughout and between organizations. More simply, IT systems manage the flow of digital information through the use of components such as business applications, data, hardware (e.g. computers, physical servers, and network equipment), and software (e.g. applications, operating systems, and virtualization capabilities). IT systems have a programmable capacity so they can be adjusted, augmented, and re-programmed in countless ways to fit the evolving networks, applications, and user needs.

International Maritime Organization (IMO) is the United Nations specialized agency with responsibility for the safety and security of shipping and the prevention of marine and atmospheric pollution by ships.[15]

Malware is malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware.

Maritime cyber risk is a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

Maritime cyberspace is a global domain consisting of the interdependent networks of IT systems, OT systems, the internet, data, the electromagnetic spectrum (EMS), and telecommunications networks used within the maritime domain on ships and at ports.

Operational technology (OT) systems refers to technology that monitors and controls specific devices and processes within industrial workflows. It carries out the function of physical processes through hardware and software that is usually designed to do specific things like control heat, monitor mechanical performance, trigger emergency shutoffs, etc. Typically, this is done through ICS and supervisory control and data acquisition (SCADA).

Patches are software and operating system updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced security features.

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing a specific, usually well-known brand, usually for financial gain.

Positioning, navigation and timing (PNT) systems are used to help understand where vessels are on the surface of the earth (positioning), to determine how to get where the vessel needs to go (navigation), and to synchronize networks or time stamping purposes.

PNT system disruptions refer to either jamming or spoofing of PNT systems.

- Jamming involves a radiocommunication jamming device, also known as a signal silencer, blocker or disabler, and designed to interfere with, disrupt, or block radiocommunication signals and services.
- Spoofing is when someone impersonates a person or a company to access sensitive information or spread malware. Spoofing can apply to various communication channels and may involve different levels of technical complexities. GPS spoofing specifically uses fake signals that are broadcasted to deceive the victim. For example, a ships receiver can be deceived with counterfeit satellite automatic identification signals generated to gain control of the navigation system taking the vessel off course or appearing in a different location.

Security by design refers to the aspect of security that is built into the technical architecture of anything that is created and should therefore be built into future life cycles.

Ship Classification Societies are non-governmental organizations that set and apply design and construction rules to ensure that vessel structures and their shipbuilders comply with those rules. Their mandate is to rate new ships based on predefined technical standards and then to assign the ships a ‘’class’’ according to their design. Class societies also offer other services, such as ship inspections and surveys, on behalf of government authorities, to ensure compliance with regulations.

Footnotes

[1] Council of Canadian Academies, The Value of Commercial Marine Shipping to Canada. Ottawa (ON): The Expert Panel on the Social and Economic Value of Marine Shipping to Canada. May 24, 2017 The Value of Commercial Marine Shipping to Canada | Clear Seas (Accessed March 24, 2022)

[2] CyberOwl, HFW Report: Maritime Industry Pays Average $3m Ransom in Cyberattacks. 22 March 2022 CyberOwl, HFW Report: Maritime Industry Pays Average $3m Ransom In Cyberattacks - Cyber Owl (Accessed 25 March 2022)

[3] Many shippers and shipyards have been hit by significant cyber attacks. It is our understanding that they now have much stronger cyber response structures. Here is a non-exhaustive list: 2022 Expeditors International, US; 2021 Bureau Veritas, France; 2021 Swire Pacific Offshore, Singapore; 2020 Vard Shipyard, Norway; 2020 Compagnie Maritime d'Affrètement (CMA) and Compagnie Générale Maritime (CGM), France; 2020 Mediterranean Shipping Company, Switzerland; 2018 Shipbuilder Austal, Australia; 2017 Maersk Shipping, Denmark; 2017 Shipbroker Clarksons, United Kingdom.

[4] In the United States, House Members have introduced the Port Crane Security and Inspection Act of 2022, which limits their exposure to cybersecurity risk in their maritime cybersecurity critical infrastructure sector owned or manufactured by foreign countries. For more information, please see Port Crane Security and Inspection Act of 2022. US Congress on the Web. January 26, 2022. https://www.congress.gov/bill/117th-congress/house-bill/6487/text?r=18&s=1 (Accessed on April 5, 2022).

[5] Deborah Haynes, Iran's Secret Cyber Files: How Cargo Ships Could be Sink, Sky News on the Web. July 27, 2021. https://news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871 (Accessed March 25, 2022).

[6] Daphne Leprince-Ringuet, "The Global Chip Shortage is Creating a New Problem: More Fake Components," ZDNet on the Web. June 9, 2021. https://www.zdnet.com/article/the-global-chip-shortage-is-creating-a-new-problem-more-fake-components-as-fraudsters-cash-in/ (Accessed March 27, 2022).

[7] International Association of Classification Societies, IACS Adopts New Requirements on Cyber Safety. 21 April 2022 IACS adopts new requirements on cyber safety - IACS (Accessed 17 October 2022)

[8] In the past 5 years, the following non-exhaustive list of ports or cargo terminals that have been hit by cyber attacks: 2022: Jawaharlal Nehru Container Terminal, India; 2021: Port of Houston, US; 2021: Port of Cape Town, Port of Elizabeth and Durban, Ngqura Port, South Africa; 2020: Port of Kennewick, US; 2020: Port of Shahid Rajee, Iran; 2020: Port of Marseilles, France; 2018: Port of Vancouver, Canada;

2018: Port of San Diego, US; 2018: Port of Barcelona, Spain; 2018: COSCO shipping at Port of Long Beach, US; 2017: Port of Rotterdam, Netherlands.

[9] In a survey conducted by a maritime cybersecurity company, more than 25% of seafarers don't know what actions would be required of them during a cyber incident. For more information, please see CyberOwl, HFW Report: Maritime Industry Payout Average $3 m Ransomware Cyberattacks. CyberOwl on the Web. March 22, 2022. https://cyberowl.io/cyberowl-hfw-report-maritime-industry-pays-average-3m-ransom-in-cyberattacks/ (Accessed April 1, 2022).

[10] J. Dafrron et al., Shen Attack: Cyber Risk in Asia Pacific Ports, Cambridge Centre for Risk Studies, 2019, https://assets.lloyds.com/assets/pdf-cyrim-shen-attack-final-report-exec-summary/1/pdf-cyrim-shen-attack-final-report-exec-summary.pdf (Accessed Jan 18, 2022).

[11] A System of systems: Cooperation on Maritime Cybersecurity, Atlantic Council on the Web. Oct 4, 2021. https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-a-system-of-systems/ (Accessed on Jan 11, 2022).

[12] It is important to align definitions on cyber. The US committee of National Security Systems as of March 2, 2022 define Maritime Cyberspace as "Maritime Cyberspace is a global domain consisting of the interdependent networks of, Information Technology (IT) infrastructure, Operational Technology (OT) infrastructure, the internet, resident data, the electromagnetic spectrum (EMS), and telecommunications networks, computers, information and communication systems, and embedded processors, and controllers related to infrastructure processes and functions."

[13] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf pg H-4

[14] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

[15] https://www.imo.org/