الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري

Arab Academy for Science, Technology & Maritime Transport

9 Marlog 2020

The International Maritime Transport and Logistics Conference "Marlog 9"

Impacts of the Fourth Industrial Revolution on Port-City Integration

"World Port Sustainability Program Aspects"

DEMONSTRATING THE CYBER VULNERABILITIES OF SIGNIFICANT MATITIME TECHNOLOHIES TO THE PORT FACILITIES AND ON BOARD OF VESSELS

Karim Mohamed Aboul-Dahab

29-31 March, 2020

Hilton Green Plaza Hotel, Alexandria - Egypt

Index

INTRODUCTION

Ships are increasingly using systems that rely on digitization, digitalization, integration, and automation, which call for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet. In 2017, the International Maritime Organization (IMO) adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS). The Resolution stated that an approved Safety Management System SMS should take into account cyber risk management in accordance with the objectives and functional requirements of the International Safety Management (ISM) CODE. The IMO encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

INTERNATIONAL
MARITIME
ORGANIZATION

INTRODUCTION

Cybersecurity introduces an additional element into the safety equation, security against deliberate actions intended to cause harm. Security has always been a concern with naval ships, and the military routinely exercise precautions to maintain the security of their ships and offshore assets. Commercial vessels routinely employ special security measures under certain circumstances to prevent theft, piracy, smuggling or stowaways.

Figure 2.2 Cyber security threat actors

INTRODUCTION

In 2012, the major Saudi Arabian state owned oil and gas company, Saudi Aramco, which provides 10 % of the global oil suffered a cyber-attack during Ramadan month. An employee of the company opened a phishing mail with an infected link. According to Abdullah al-Saadan, vice president for corporate planning of Aramco, the primary intention behind this attack was to stop the flow of oil and gas to the international and national market (Reuter, 2012).

In August 2011,The Islamic Republic of Iran Shipping Lines (IRISL), an Iranian state-owned shipping company, fell victim to a cyber attack. Lars Jenson, founder of CyberKeel ,reported, “The attacks damaged all the data related to rates, loading, cargo number, date and place … resulting in severe financial losses

Literature Review

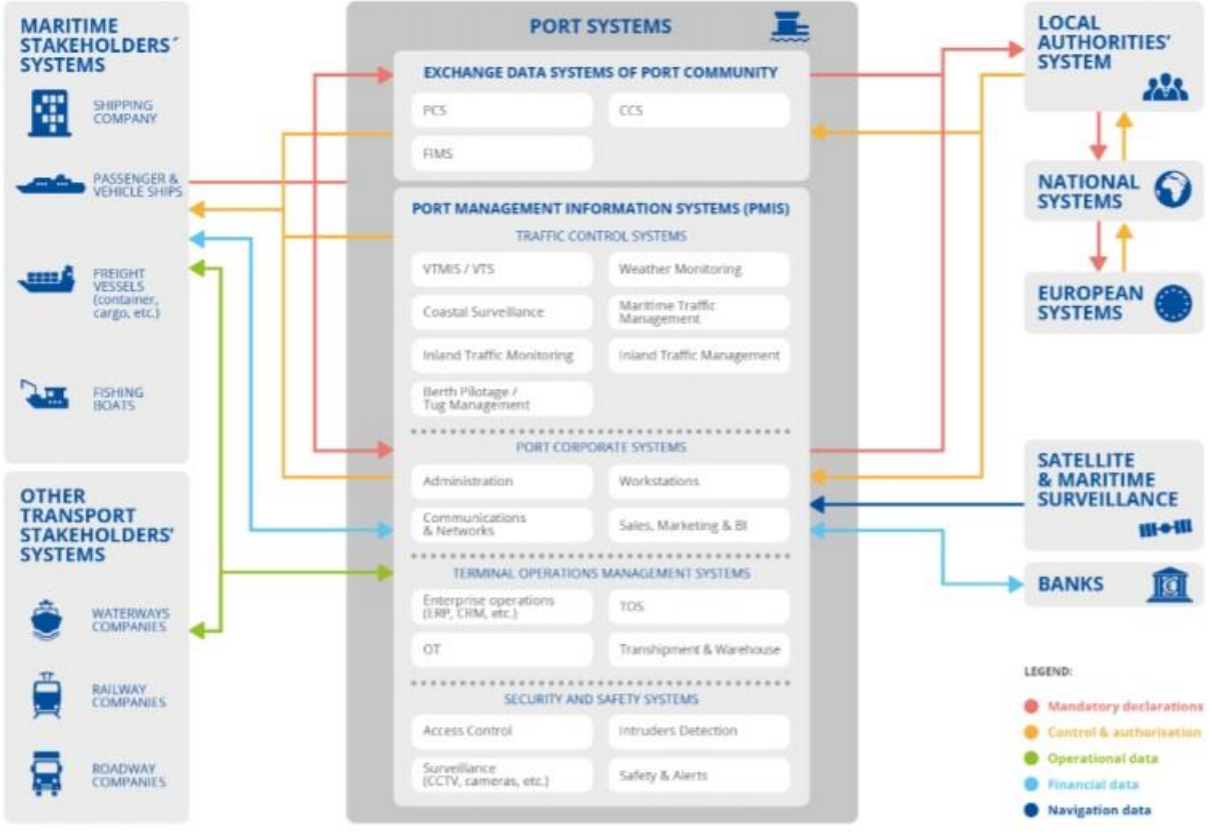
The topic of cybersecurity within the maritime industry is as dynamic as any other sector of business. The industry's global reach, large volume of capital transactions, extensive use of commercial services, and reliance on information technology create significant opportunities for exploitation through the cyber domain , Security threats have evolved from coastal piracy to complex smuggling operations, transnational organized crime, and terrorism. Safety risks have likewise evolved as merchant shipping progressed from sailing ships to ships driven by coal-fired steam boilers, to diesel engines and most recently to liquefied natural gas. Waterfront operations evolved from break bulk cargo to containerization, with sophisticated systems now controlling the movement and tracking of containerized and liquid cargo

Cyber Security on Port Facilities

The growth of digitalization and the connectedness produce pressure on the industry to be more and more connected. shipping companies, vessels ,ports and terminals tend to install similar software to load ,unload and track cargo , the absolute dependency of systems and equipment regarding interconnectivity operations creates more vulnerability and representing an increase in opportunities for cyber-crimes ,so the vulnerability of a one single software installed could cause significant damages to other vessels, ports, terminals and shipping companies consequently.

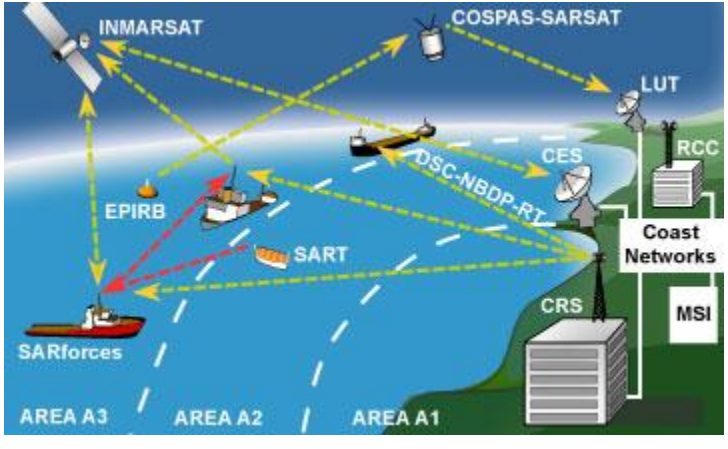
GPS technology, coupled with geographic information system (GIS) software, is a key to the efficient management and operation of automated container placement in the world's largest port facilities. GPS facilitates the automation of the pick-up, transfer, and placement process of containers by tracking them from port entry to exit. The most likely GPS maritime threat scenarios could be Jamming of a port

Port Facilities Systems



Cyber Security on board of vessels

Today's mariners rely heavily on networks, systems, and outside sources for navigation. Many significant cyber threats are the result of vulnerabilities in equipment carried and used by the maritime industry worldwide. Equipment vulnerable to cyberattacks includes navigation systems



A cyber-attack on a GMDSS system devices could manipulate the ship information details such as cargo, position and speed or sending false warnings, alarms and distress signals, jamming or disruption on any of these essential navigation systems becomes a severe problem that can affect the maritime industry, Cyber-attack on vessels are very dynamic depending on cargo, geographic position, shipborne technology and competence of the crew.

Cyber Security on board of vessels

The connected devices include the navigational system, communication system, cargo management system, engine system, dynamic system, terminal management system, tracking system, logistic system and many more. However the growth of the connected devices results in high risk fc the maritime industry, increasing the vulnerability of all th integrated bridge, engine, cargo, communication and lanc systems mentioned. For that reason, it is necessary that th maritime sector evaluates the vulnerabilities in the sophisticated and interconnected systems, which are incorporated in daily operations, and understand the complexity of maritime system vulnerabilities

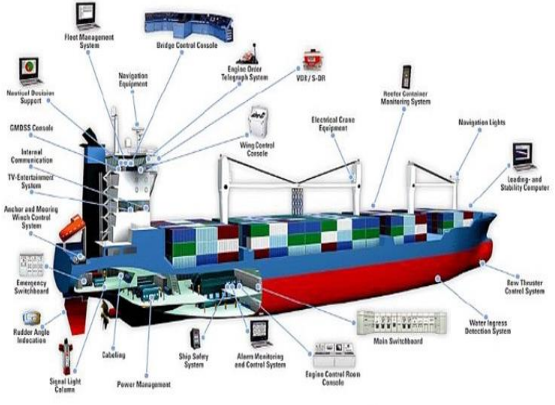


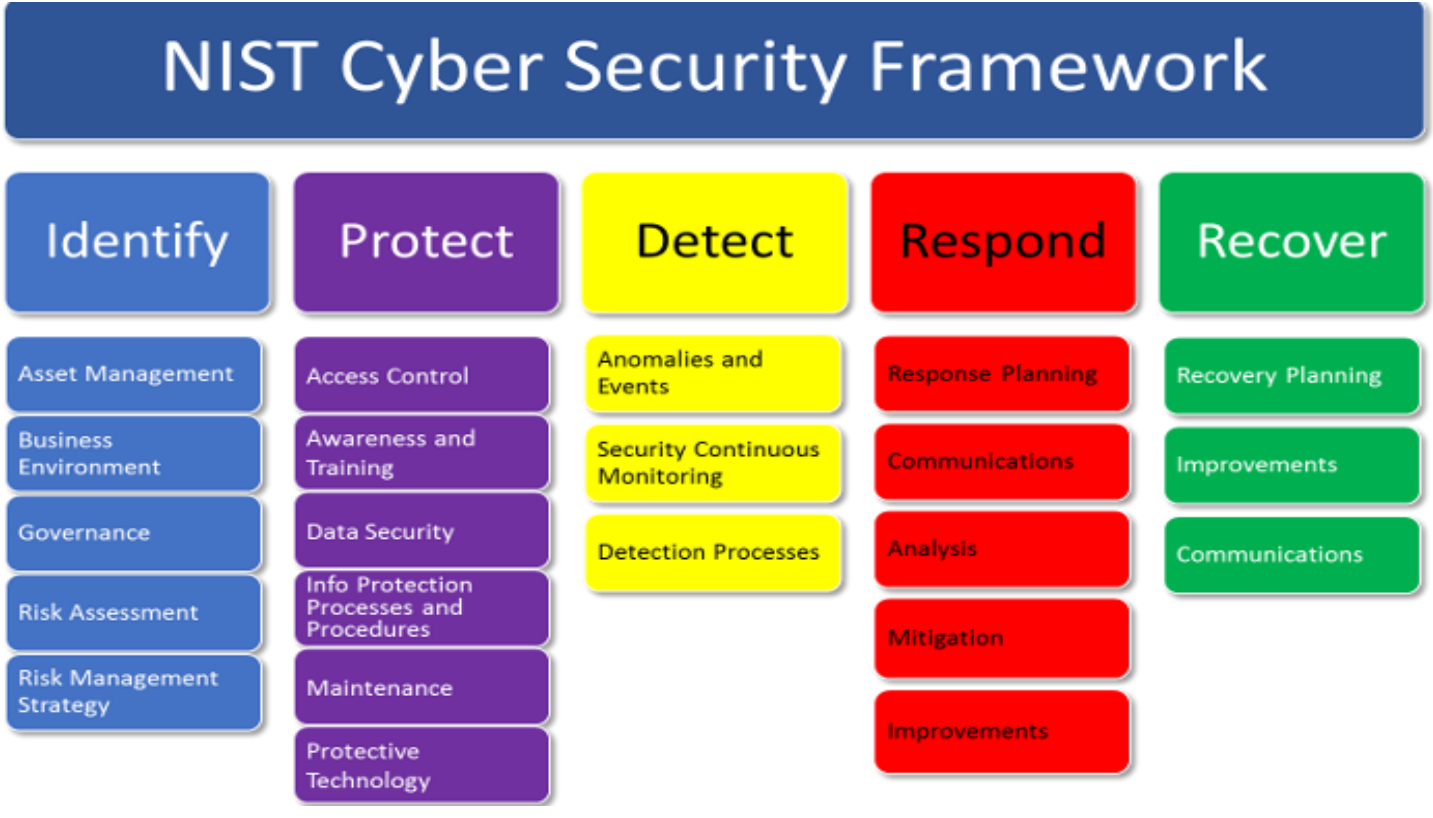
FIGURE I—TYPICAL SHIPBOARD ICS[22]

Cyber Security on board of vessels

While the intended purpose of AIS was to avoid vessel collisions, today AIS is used for several cyber-physical applications, including identification, search and rescue operations, accident investigation, remote tracking, ocean currents estimation, and the protection of marine Critical Infrastructures (CIs) same Source However, being designed in the 80s, AIS does not support any security property, such as authentication and confidentiality. Which could lead to the spoofing, hijacking, data manipulation, and Denial of Service (DoS). An attacker could: (i) create fake vessels; (ii) inject false ship details (e.g., position, speed, and Mobile Maritime Service Identity (MMSI)); (iii) impersonate vessels or port authorities; (iv) inject false information (e.g., false man-in-water alarms); and, finally, (v) send false collision warning alerts

Cyber Security Models and policies

Cyber Security Models and policies



Cyber Security Models and policies

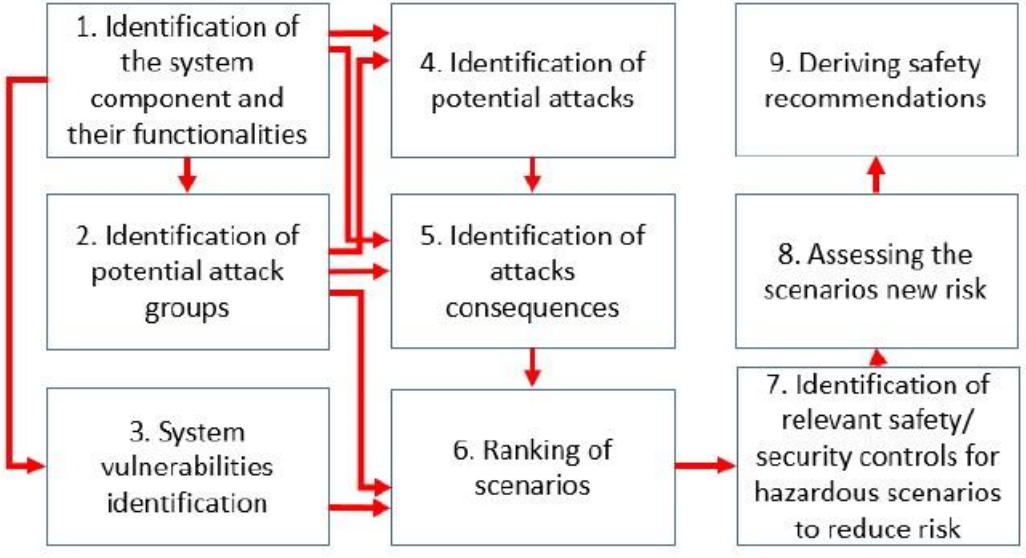


Figure 1 CPHA methodology flowchart.

Conclusions

This paper has investigated the cyber vulnerabilities of significant maritime technologies and evaluated the different frame works and guidelines on maritime cyber risk management.

The main challenges currently facing the port facilities to implement cyber security measures are 1-Lack of digital culture in the port ecosystem 2- Lack of awareness and training regarding cyber security: 3- Lack of time and budget allocated to cyber security: 4- Lack of human resources and qualified people regarding cyber security matters:

The maritime vessels have become especially reliant on GNSS technology , The vast majority of vessels now rely on (GNSS) which could be spoofed or blocked causing disrupt of navigation, GNSS signals could be vulnerable to the following threats ;Jamming and Interference by broadcasting a stronger signal that intentionally or unintentionally blocks or impacts a GNSS satellite signal.

Conclusions

From the security perspective, commercial vessels rely on civilian GNSS signals, Unfortunately, to boost message availability at the receivers, the civilian GNSS was designed to transmit messages in clear-text, without relying on any confidentiality nor authentication mechanism.

The consequences of an attack against this industry could be huge , Hence the Maritime Safety Committee (MSC) and The Facilitation Committee (FAL) have issued “Guidelines on maritime cyber risk management” (MSC-FAL.1/Circ.3) , In deed have completely accepted the NIST framework five key elements.


ANY
QUESTIONS?