RMN SEA POWER CENTRE ONLINE COMMENTARY ON MARITIME ISSUES

SUAR 3/23 1 APR 2023

SUAR is an online platform for Royal Malaysian Navy Sea Power Centre (RMN SPC) to articulate views on issues and developments in the maritime domain. The views expressed are the author's own and not necessarily those of the RMN SPC. For further information on SUAR please visit https://pusmas.navy.mil.my

GLOBAL MARITIME SECURITY ISSUES

By Lt Ts. Mohamad Aznan bin Mohd Najib RMN
RMN Submarine Training Centre

INTRODUCTION

The safety and security of ships, their crews, and cargo in international waters are global maritime security. Piracy and armed robbery, smuggling and trafficking, terrorist attacks, cybersecurity, and environmental threats are some major global maritime security issues. To address these security concerns, international organizations, governments, and industry groups are collaborating to implement security measures and increase international cooperation and information sharing.

Piracy and armed robbery at sea are serious crimes that pose a threat to global maritime security. Piracy is a robbery or criminal violence committed on the high seas outside the jurisdiction of any state. Armed robbery at sea refers to the theft of a ship's cargo or valuables by armed individuals while the ship is at sea. Although much emphasis has been on the severity of piracy activity in the Gulf of Guinea, the Southeast Asian and Western Indian Ocean regions have been exposed to piracy and armed robbery on vessels, demonstrating that such incidents are not restricted only to known "high-risk areas" regions. The IMB piracy and armed robbery report of September 2021 (Q3) released the following statistics for January to September 2021. Ninety-seven vessels have reported incidents to the IMB PRC in the first nine months of 2021. Under the definitions of piracy and armed robbery at sea, 85 vessels were boarded, nine reported attempted attacks, two were fired upon, and one was hijacked. In 25% of the reported incidents, the crew was directly impacted, with 51 crew reported kidnapped, eight taken hostage, five threatened, three injured, two assaulted, and one killed. Twenty-eight incidents were reported within the Gulf of Guinea (GoG) region in the first nine months of 2021, including the kidnapping of one crew member and 31 crew taken in five separate incidents. It is noticeable that all Q3 2021 incidents occurred at port anchorages, whereas for Q3 2020, the average distance from shore of the successful kidnappings was 100 NM, with the furthest almost 200 NM out. There has been a sustained lull in reported piracy incidents off the coast of Somalia and the more expansive Indian Ocean leading to the shipping industry reducing the designated High-Risk Area (HRA). However, on October 16, an Iranian warship prevented an attack by pirates against two oil tankers that it was escorting in the Gulf of Aden. This would make the 6th reported approach in the region within 2021. IMB's data reported incidents of armed robberies at ports in South and Central America and the Caribbean, typically linked to drug trafficking. There were also reported attacks on offshore support vessels operating in the southern rim of the Gulf of Mexico. Callao anchorage in Peru continues to be an area of concern, with 15 incidents reported in 2021, the highest number of reported incidents since 1991. While also viewed as low-level opportunistic thefts, knives were reported in 60% of the incidents. Three crewmembers were taken hostage, and over 30% involved assaults and threats to the crewmembers. All vessel types are targeted. In Singapore Straits, 41 incidents have been reported from vessels transiting the Singapore Straits since January 2021, with the highest number recorded since 1991. Although classified as low-level opportunistic thefts, the perpetrators continue to pose an immediate risk to seafarers and vessels underway. In Indonesia, there was a noticeable reduction in the number of reported incidents in Indonesian waters, with ten low-level reported incidents up to October 2021 compared to 23 incidents in 2020.

Eleven incidents have been reported in the Philippines from container vessels boarded while anchored in Manila Bay, Philippines, from January to October 2021. The ReCAAP ISC is concerned with the increasing number of incidents in the Singapore Strait. Since January 2021, there has been a growing cluster of incidents off Tanjung Pergam, Bintan Island (25 incidents), and an increase of incidents off Nongsa, Batam Island (9 incidents). The ReCAAP ISC has issued seven Incident Alerts (the latest alert on December 2, 2021), warning the maritime community of continued incidents in the Singapore Strait and the possibility of further incidents. This includes six reported incidents on board vessels underway in the Singapore Strait from November 1 to December 1, 2021. Five incidents occurred in the Traffic Separation Scheme (TSS) eastbound lane, and one incident in the precautionary area. As the perpetrators are not arrested, there is a possibility of further incidents in the Singapore Strait.[1,2]

Smuggling and trafficking describe the illegal movement of goods, people, and other contraband across national borders. These activities endanger global maritime security because they undermine state authority and contribute to organized crime and terrorism. Drug trafficking is one example of smuggling and trafficking via the maritime domain. Cocaine, heroin, and methamphetamine are frequently smuggled into countries through the seas, taking advantage of the large volumes of international trade and the ease with which ships can be disguised or concealed. Human trafficking is a severe problem in many parts of the world, with victims being transported across international waters for forced labor or sexual exploitation.

Furthermore, illicit arms are smuggled into countries via the seas for armed conflict or criminal activity. International organizations and governments have taken steps to address the issue of maritime smuggling and trafficking. The UN Office on Drugs and Crime (UNODC) has established a Global Maritime Crime Program to strengthen countries' capacity to combat organized crime in the maritime environment. The International Maritime Organization (IMO) has also established the Joint Maritime Information and Coordination Centre (JMICC), which promotes information sharing and cooperation among countries to combat the threat of smuggling and trafficking at sea. [3, 4]

Terrorist attacks in the maritime domain are acts of violence committed by extremist groups, such as bombings, hijackings, and other forms of aggression, with the intent of causing harm, destruction, and widespread fear. Because of the potential impact on commerce, trade, and the flow of goods and people, these attacks pose a significant threat to global maritime security. Terrorist attacks in the maritime domain include the MV Limburg. Terrorists attacked the French-flagged oil tanker MV Limburg off the coast of Yemen in 2002, killing one crew member and causing a massive oil spill. The Mumbai attacks Terrorists attacked multiple locations in Mumbai, India, in 2008, including the city's main port, the Taj Mahal Palace hotel, and other tourist attractions. The MV Iceberg Pirates kidnapped the crew of the MV Iceberg, a Liberian-flagged cargo ship, in 2011 and held them hostage for over a year. To combat the threat of terrorism in the maritime domain, international organizations, governments, and industry groups are collaborating to improve security measures, improve information sharing and cooperation, and develop response plans for potential terrorist incidents. The

International Maritime Organization (IMO) established the International Ship and Port Facility Security (ISPS) Code, which establishes minimum security standards for ships and port facilities, while the International Chamber of Commerce (ICC) established the Commercial Crime Services (CCS), which provides information and assistance to ships and their crews in avoiding and responding to terrorist attacks. [1, 2]

Cybersecurity is not just about preventing hackers from accessing systems and information. It is also about protecting digital assets and data, ensuring business continuity, and ensuring the maritime industry is resilient to external and internal threats. It is crucial to keep ship systems safe from physical attacks and to ensure the integrity of supporting systems. The complexities associated with vessels and tankers make them vulnerable to high-impact attacks. Cyber incidents can last for hours, days, or weeks. When one ship is impacted, it can often spread malware to sister's vessels via the corporate network. Some of the potential attacks that can cripple a vessel's operations include an attack on an OEM network or third-party supplier that spreads to their client's on-vessel OT network, an attack on a satellite provider that gains access to a vessel's IT/OT network, exploited cyber vulnerabilities that grant access to a vessel's OT network and provide various attack options (GPS/navigation system attack, Open/close critical valves, Propulsion and rudder control, Ballast control, Ransomware/Malware and Gain full administrative privileges. A compromised ship system could initiate physical harm to the IT and OT systems, personnel, and cargo, potentially endangering lives or causing the ship's loss and sensitive information, including commercially sensitive or personal data. Cybersecurity attacks are not new in the maritime industry, but many incidents go unreported. There is an ongoing reluctance to share critical information with law enforcement agencies and collaborate with peers to share threat information to thwart future attacks and build cybersecurity best practices. With maritime cyberattacks increasing by 900% since 2017, the number of reported incidents is set to reach a record by the end of 2020.

A sampling of cyberattacks affecting the maritime industry in 2020 shows that all organizations can be susceptible to attack, regardless of size or location. One of the most significant and devastating cyberattacks to date is NotPetya, which caused more than $10 billion in total damages in June 2017. Primarily targeted at Ukrainian companies, NotPetya's reach went far beyond Ukraine and hit many large organizations, including pharmaceutical company Merck, delivery company FedEx and Danish shipping giant Maersk (A.P. Møller-Maersk), which handles one out of seven containers shipped globally. Maersk was hit particularly hard, to the tune of $300 million, and lost most of its data, including all end-user devices, including 49,000 laptops and print capability, were destroyed, all of their

1,200 applications were inaccessible, and approximately 1,000 were destroyed, data was preserved on back-ups, but the applications themselves could not be restored as they would be reinfected, 3,500 of their 6,200 servers were destroyed. They could not be reinstalled, all fixed-line phones were inoperable due to the network damage, and because they had been synchronized with outlook, all contacts had been wiped from mobiles, severely hampering any coordinated response. More recently, with the onset of the COVID-19 pandemic, the number of shipping cyberattacks has jumped 400% since February. Travel restrictions, social distancing, and the economic recession impact the maritime industry and its ability to protect itself. OEMs, technicians, and vendors are forced to connect standalone systems to the Internet to service them. Ship and offshore staff are connecting their OT systems to onshore networks for brief periods to carry out diagnostics and upload software updates, leaving endpoints, critical systems, and components susceptible to attack since they are no longer segmented. Also, the stress levels of short-staffed crews can leave vessels vulnerable to scams, misconfigurations, and human error. [7, 8]

The environmental threats in the maritime domain refer to the potential harm caused to the marine environment and its wildlife, including air pollution, water pollution, and acoustic and oil pollution. Ships are responsible for more than 18 percent of some air pollutants. It also includes greenhouse gas emissions. The International Maritime Organization (IMO) estimates that carbon dioxide emissions from shipping were equal to 2.2% of the global human-made emissions in 2012 and expects them to rise 50 to 250 percent by 2050 if no action is taken. According to shipping researcher Alice Bows-Larkin, there is a perception that cargo transport by ship is low in air pollutants because it is the most efficient transport method for equal weight and distance. This is particularly true in comparison to air freight. However, because sea shipment accounts for the far more annual tonnage and the distances are often large, shipping's emissions are globally substantial. A difficulty is that the increasing amount of shipping overwhelms gains in efficiency, such as from slow-steaming or using kites. The tonne-kilometers of sea shipment growth has averaged 4 percent yearly since the 1990s, and it has grown by a factor of 5 since the 1970s. There are now over 100,000 transport ships at sea, of which about 6,000 are large container ships. The fact that shipping enjoys substantial tax privileges has contributed to the growing emissions. Ballast water discharges by ships can harm the marine environment. [9] Cruise ships, large tankers, and bulk cargo carriers use a considerable amount of ballast water, often taken on in the coastal waters in one region after ships discharge wastewater or unload cargo and discharge at the next port of call, wherever more cargo is loaded. [10] Ballast water discharge typically contains various biological materials, including plants, animals, viruses, and bacteria. These materials often include non-native, nuisance, invasive, and exotic species that can cause extensive ecological and economic damage to aquatic ecosystems and severe human health problems. The cruise line industry dumps 255,000 US gallons (970 m^3) of greywater and 30,000 US gallons (110 m^3) of blackwater into the sea every day. [9] Blackwater is sewage, and wastewater from toilets and medical facilities, which can contain harmful bacteria, pathogens, viruses, intestinal parasites, and harmful nutrients. Discharges of untreated or inadequately treated sewage can cause bacterial and viral contamination of fisheries and shellfish beds, producing risks to public health. Nutrients in sewage, such as nitrogen and phosphorus, promote excessive algal blooms, which consume oxygen in the water and can lead to fish kills and the destruction of other aquatic life. A large cruise ship (3,000 passengers and crew) generates an estimated 55,000 to 110,000 liters per day of blackwater waste. [11] Greywater is wastewater from the sinks, showers, galleys, laundry, and cleaning activities aboard a ship. It can contain various pollutant substances, including fecal coliforms, detergents, oil and grease, metals, organic compounds, petroleum hydrocarbons, nutrients, food waste, and medical and dental waste. Sampling done by the EPA and the state of Alaska found that untreated greywater from cruise ships can contain pollutants at variable strengths and contain levels of fecal coliform bacteria several times greater than is typically found in untreated domestic wastewater. [12] Greywater can cause adverse environmental effects because of concentrations of nutrients and other oxygen-demanding materials. Greywater is typically the largest source of liquid waste generated by cruise ships (90 to 95 percent of the total). Estimates of greywater range from 110 to 320 liters per day per person or 330,000 to 960,000 liters per day for a 3,000-person cruise ship. [13] MARPOL Annex IV was brought into force in September 2003, strictly limiting untreated waste discharge. Modern cruise ships are most commonly installed with a membrane bioreactor type treatment plant for all black and greywater, such as G&O, Zenon, or Rochem bioreactors, producing near drinkable quality effluent to be re-used in the machinery spaces as technical water.

In conclusion, global maritime security is a complex issue that encompasses a range of challenges, including piracy and armed robbery, smuggling and trafficking, terrorist attacks, cybersecurity, and environmental threats. These threats pose a significant risk to the safety and security of ships, ports, and other related infrastructure. They can have long-lasting impacts on the marine environment and the livelihoods of people who depend on it. To address these challenges, international organizations, governments, and industry groups are working together to implement best practices, regulations, and response plans to ensure the safety and security of the global maritime domain. Adequate global maritime security requires a multi-faceted approach that includes cooperation, information sharing, and the development of technologies and strategies to enhance resilience and mitigate risk.

References:

1. International Maritime Organization (IMO). (n.d.). Piracy and Armed Robbery against Ships.

2. International Chamber of Commerce (ICC). (n.d.). Commercial Crime Services.

3. United Nations Office on Drugs and Crime (UNODC). (n.d.). Global Maritime Crime Programme.

4. International Maritime Organization (IMO). (n.d.). Joint Maritime Information and Coordination Centre (JMICC).

5. International Maritime Organization (IMO). (n.d.). Guidelines for Cybersecurity Management for Ships and Port Facilities.

6. International Association of Classification Societies (IACS). (n.d.). Common Structural Rules (CSR).

7. Walker, Tony R.; Adebambo, Olubukola; Del Aguila Feijoo, Monica C.; Elhaimer, Elias; Hossain, Tahazzud; Edwards, Stuart Johnston; Morrison, Courtney E.; Romo, Jessica, et al. (2019). "Environmental Effects of Marine Transportation ."World Seas: An Environmental Evaluation. pp. 505–530. doi:10.1016/B978-0-12-805052-1.00030-9. ISBN 978-0-12-805052-1.

8. Urbina, I. (September 25, 2019). "Dumping into the Ocean The Outlaw Ocean.".

9. The Ocean Conservancy, "Cruise Control, A Report on How Cruise Ships Affect the Marine Environment," May 2002, p. 13. - PDF [1]

10. EPA Draft Discharge Assessment Report, pp. 3-5–3–6.

11. Cruise Control, p. 15.