National Maritime Foundation

India STRATEGIC

The Indian Navy

Perspectives and Technologies

NMF - India Strategic Yearbook 2019

Maritime Cybersecurity

Munish Sharma

GLOBALIZATION has led to an extensive movement of trade, commerce, capital, ideas and people. This process has been facilitated by the maritime and cyber domains that have played a key role in integrating markets, businesses and people for both economic and social growth. Sea based commerce is the backbone of industrialized economies, and accounts for close to 90 percent of the global trade and movement of goods. Communication and navigation needs of ships are critically dependent on smart information systems, and so are the business operations of shipping corporations. Information Communication and Technology (ICT) enables essential maritime operations in a number of ways such as navigation, propulsion, freight management, and traffic control communications.[1] Furthermore, safe and secure ports and shipping operations are essential to the maritime industry. For instance, the 2017 NotPetya malware attack resulted in disruptions in operations with adverse implications for the global supply chain. In the aftermath of the NotPetya attack, Cybersecurity received unprecedented attention in the commercial maritime world. Cybersecurity in the maritime domain has two key aspects, on-shore looking at the safe operations of ships, and off-shore for safe business operations of shipping enterprises and terminal operators.

Maritime Cybersecurity Risks

Security of maritime interests of the nation states and good order at sea has been at the core of the United Nations and the affiliated organizations. The International Maritime Organization (IMO) – a permanent international body to promote maritime safety and security – has introduced a number of measures to ensure safety of the maritime space. Technology has been a key enabler for security systems such as International Ship and Port Facility Security[2] (ISPS) code, Global Maritime Distress and Safety System[3] (GMDSS), Automatic Identification System[4] (AIS), and Long-Range Identification and Tracking[5] (LRIT) system. These systems use satellites, radios and microwave communication for data transmission, complex hardware and precisely developed software. At the ship end, all the above systems, including the Global Positioning System (GPS) and the Electronic Chart Display and Information Systems (ECDIS),[6] Electronic Navigation Chart (ENC), Voyage Data Recorder (VDR), Dynamic Positioning (DP) etc. are vulnerable to interference and disruption. On-shore operations, such as cargo management, cargo handling, loading and unloading etc. and ship-tracking are a soft target. On-board networked Information Technology (IT) and Operational Technology (OT) widen the attack surface of the ship. Some of the IT and OT systems, meant for monitoring, data collection, maintenance, safety and security are remotely accessible; and it could be a possible gateway to the security perimeter of the ship.

The common vulnerabilities, from cyber point of view, are as diverse as obsolete operating systems, outdated antivirus, default security configurations and weak access control, inadequate segmentation of networks, un-patched applications or operating systems, and neglecting best practices or implementation of guidelines even at the end of the third parties such as contractors and service providers.[7] The various functions, which could be subject to cyber attack are the cargo handling and management systems; shipment-tracking; propulsion, steering, power control and performance management systems of the ship; public networks of shipping companies, and their respective administrative and communication systems. These certainly include the on-board Supervisory Control and Data Acquisition (SCADA) systems, which underpin the aforementioned functions of a seaborne platform – be it a cargo ship or a warship - destroyer, frigate, or even an aircraft carrier for that matter.