

**Maritime Cybersecurity is an emerging area of concern for India as cybersecurity still does not attract the attention it needs in the maritime domain and its assets.**

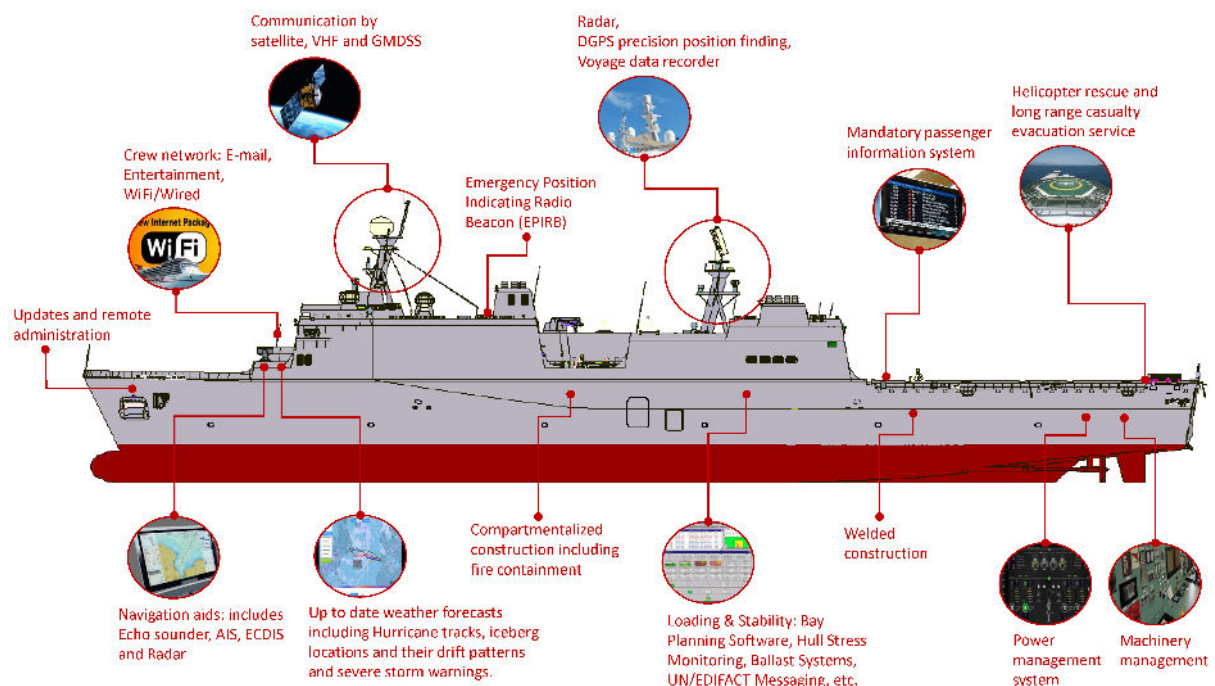
Image courtesy, Aquilon

## Maritime Cyber Security Challenges: Strategies for Resilience

by Cdr. Satyajit Roy

### Introduction

In the vast expanse of the world's oceans, the maritime industry serves as a vital lifeline for global trade, transportation and commerce. Yet, as ships navigate through the digital era, they encounter a new set of challenges posed by cyber threats. Maritime cyber security has emerged as a critical concern, necessitating a proactive approach to safeguarding vessels, ports, and maritime infrastructure against malicious actors.



(Image courtesy CyberEvolve)

### Maritime Industry Overview

The maritime industry, comprising shipping companies, ports and related service providers, plays a pivotal role in facilitating international trade, with over 90% of global trade transported by sea. Over the years, technological advancements have revolutionized maritime operations, introducing automated systems, digital communication networks, and remote monitoring capabilities. However, this digital transformation has also exposed the industry to cyber security risks, as interconnected systems become susceptible to cyber attacks.

### The International Safety Management (ISM) Code, supported by the International Maritime Organization (IMO) Resolution MSC. 428(98).

The Code and resolution stands as a cornerstone in ensuring the safety and security of maritime operations worldwide. Enacted in response to a series of maritime accidents in the late 20th century, the ISM Code sets forth comprehensive guidelines and standards for the management and operation of ships, emphasizing the importance of a safety management system (SMS) to identify, assess, and mitigate risks at sea. Resolution MSC. 428(98) further enhances the implementation and enforcement of the ISM Code, providing a framework for flag states, classification

*Acknowledgements & Sources: Aquilon, Naval Communications, Maritime Cyber Security, OSInt,*