MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

Digital Blue Zone: Ensuring Maritime Cyber Security

Adil M. Siddiqui

October 10, 2024

Summary

The formulation of a National Maritime Cyber Security Framework involving the armed forces, civil authorities like CERT and NCIIPC and the private sector is required to counter the ever-evolving landscape of cyber security threats in the maritime domain. Safeguarding shore-based information technology assets is vital towards ensuring the cyber security of supply chains.

In the age of disruptive technologies such as cloud computing and Artificial Intelligence, new dimensions of warfare pose unique challenges. Many nation states are increasingly resorting to these warfare domains to inflict attacks with the help of non-state actors. Amongst these, the most potent domain, especially for non-state actors, is Cyber Warfare. The criticality of the maritime domain for a nation's economy cannot be overlooked. It serves as a vital conduit for trade, energy security and resource exploitation. India's maritime domain, for instance, encompassing its extensive coastline, exclusive economic zone (EEZ), coupled with its strategic location in the Indian Ocean Region (IOR), offers immense economic potential but also poses unique maritime security challenges. Over 95 per cent of India's trade by volume and 70 per cent by value is transported by sea.[1] Hence, the maritime domain is a critical asset for a country, making it a potential target for the adversary to exploit.

Maritime Cyber Warfare

Maritime Cyber Attack Database (MCAD), maintained by NHL Stenden University of Applied Sciences, Netherlands, lists over 160 cyber incidents involving the maritime sector in the ongoing Russia–Ukraine war. With Automatic Identification System (AIS) and Global Positioning System (GPS) spoofing, British and Dutch NATO warships seemed within 12 Nm of the Crimean coast on 24 June 2021 necessitating warning firings whilst it turned out to be a virtual trip that never took place. Surprisingly, these ships were anchored 300 km away in Odessa, Ukraine. The simulated naval attack was executed to provoke a reaction through deployment of Disruptive Cyber Maritime Power.[2]

During the last week of December 2023 and the first week of January 2024, GPS disruptions were reported in Poland, Sweden, Finland, Estonia and Latvia (Automatic Dependent Surveillance-Broadcast, (ADS-B system) by ships and aircraft operating over the Mediterranean and the Black Sea. These maritime cyber-attacks of AIS and GPS spoofing, manipulation and jamming were categorised as 'Deceptive Practices'.[3] In the Middle East, the US carried maritime cyberattack on Iranian Warship MV Behshad in February 2024 to impede the warship from sharing intelligence about location of various cargo vessels in Red Sea and Gulf of Aden with Houthi rebels.[4] NotPetya, a malware, caused damage worth US$ 300 million to shipping company

[1] **"Ports & Shipping Industry in India"**, , Invest India.

[2] Tom Bateman, **"HMS Defender: AIS Spoofing is Opening Up a New Front in the War on Reality"**, *Euro News*, 28 June 2021.

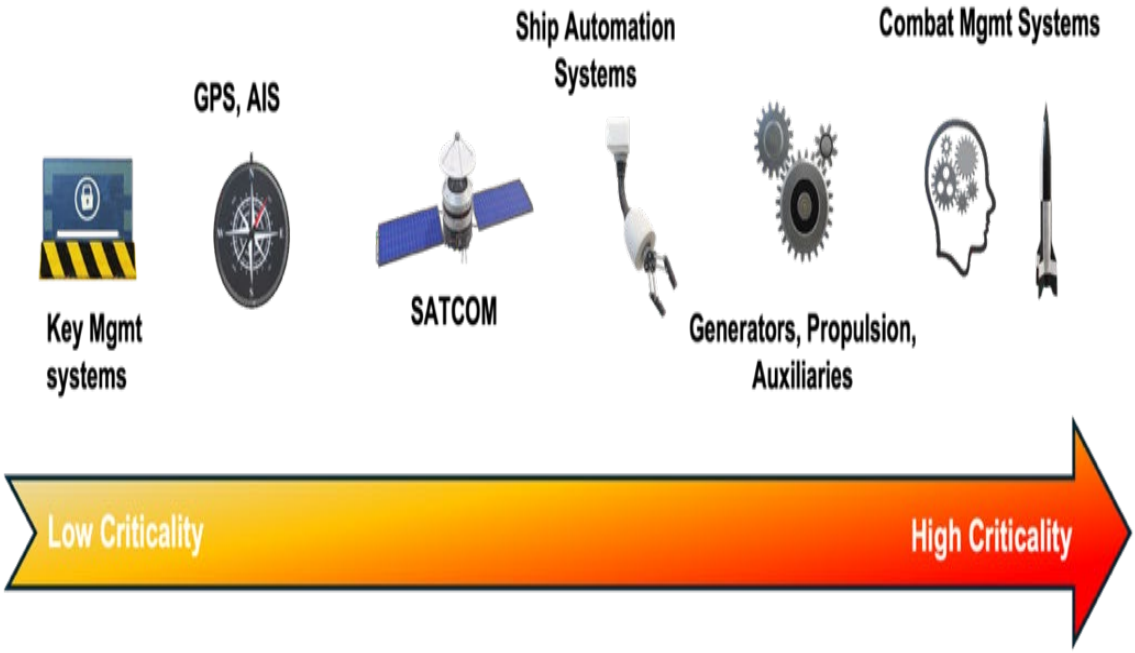
[3] Jeremy Hsu, **"Unprecedented GPS Jamming Attack Affects 1600 Aircraft Over Europe"**, *NewScientist*, 29 March 2024.

[4] **"U.S. Conducted Cyberattack on Suspected Iranian Spy Ship"**, *NBC News*, 15 February 2024

Maersk based in Denmark in addition to re-installation of 45000 PCs and replacement of 4000 servers for recovery.[5]

Maritime infrastructure uses digital networked systems allowing real-time sharing of information with other shipboard and shore-based systems using commercial satellite and shore-based Radio Frequency (RF) or terrestrial Optical Fibre Communication (OFC) network. Naval infrastructure is predominantly the same with secure and encrypted standalone satellite and RF/OFC network for naval communication ensuring seamless operation. The naval infrastructure could use the commercial set-up whilst the converse is not permitted. The digital maritime landscape relies heavily on services like navigation, weather warnings and Global Maritime Distress and Safety System (GMDSS). While AI and automation are driving innovation in maritime industry, they also create potential vulnerabilities that could be exploited by cybercriminals. Various threat vectors with regard to cyber security on the basis of criticality can be segregated as follows:[6]

Figure 1: Cyber Threat Landscape on board Marine/ Naval Ships

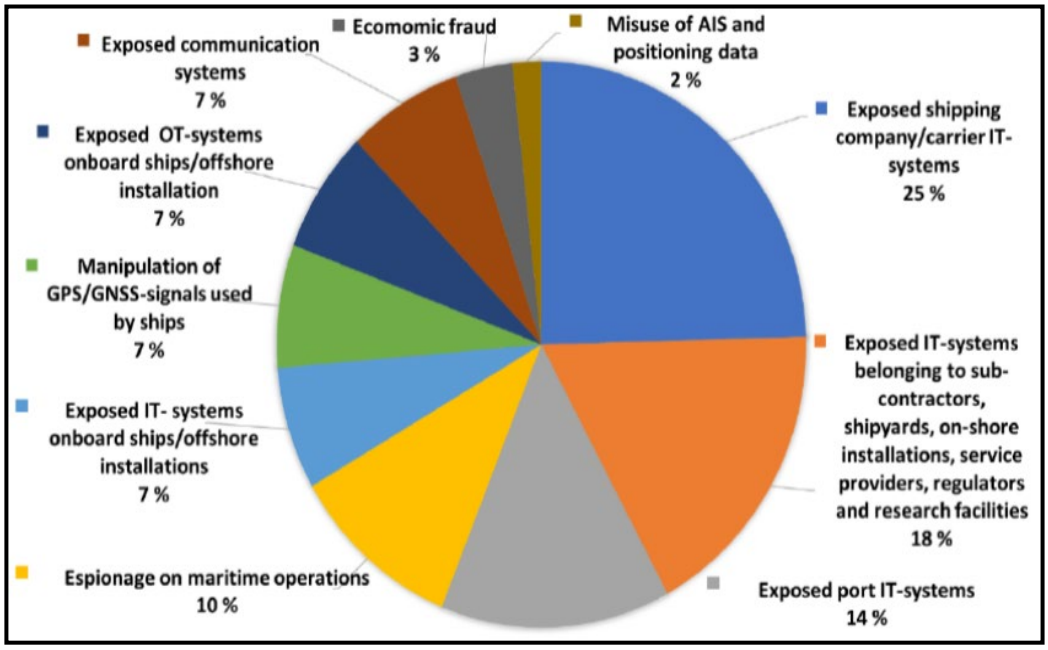


Source: Author

[5] Namita Barthwal and Commander (Dr) Nitin Agarwala, **"Industry 4.0 in the Shipping Industry: Challenges and Preparedness – The Prevailing Scenario"**, National Maritime Foundation, 24 July 2020, p. 270.

[6] A merchant or a naval ship contains a range of systems like a Key Management system, Navigational suite having AIS, GPS, Navigation Radars, satellite communication systems like INMARSAT, various automation systems for cargo control, Propulsion and Power distribution systems along with auxiliary machineries and Combat Systems like Medium/Long Range missiles and Main Gun in Naval Platforms.

Figure 2: Cyber Threat Pie Chart (2010–2020)



Source: P.H. Meland et al., **"A Retrospective Analysis of Maritime Cyber Security Incidents"**, *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, Vol. 15, No. 3, 2021, pp. 519–30.

The usage of AI and automation have revolutionised the civil and military maritime domain, made sea routing predictive and safe, made deliveries faster, business profitable and finally resulted in more expeditious and reliable military operations. It has led to a technological race towards adoption of AI-based solutions in every domain. Maritime industry and global navies around the world are exploring and implementing AI-based solutions in areas such as machinery fault prediction, asset deployment matrix, machinery performance trending, inventory management to augment op-logistics, real-time platform classification, drone swarm control and coordination and operational decision-making.

However, this exponential growth has presented the world with new challenges. Cyber security and AI/ML systems are not exactly great companions. A learning system, either machine learning or deep learning, is different from a traditional software application with issues like reliability of training data, Blackbox logic, no guarantee of desired performance for all possible inputs, fear of reverse engineering, etc. Further, possibility of an adversarial AI attack has transcended the realms of science fiction and is a potent mode of mission disruption. This technology is increasingly being used to fool the learning models in fields of image recognition or voice recognition or object classification, thus resulting in undesired outputs. Implications in the field of autonomous ships or maritime surveillance or maritime navigation are indeed of concern.

Maritime Cyber Security Initiatives: Global Scan

Recognising the urgent need towards battling cyber security threats to maritime domain, the International Maritime Organisation (IMO) adopted Resolution MSC.428(98) in June 2017[7] and further issued Guidelines on Maritime Cyber Risk Management, Ver 2.0 in April 2022. The highlights of the above guidelines and other notable global initiatives are listed in Table 1.

Table 1: Global Maritime Cyber Security Initiatives

S. No.	Guidelines/Strategy	Key Highlights
(a)	US National Maritime Cyber Security Plan, 2020[8]	The document highlights the need to prioritise cyber security measures in Maritime Transportation System (MTS), highlights various cyber security risks and the need for maintenance of standards, the importance of information and intelligence sharing, development of maritime cybersecurity workforce and international cooperation.
(b)	IMO Guidelines on Maritime Cyber Risk Management, Ver 2.0, 2022[9]	These guidelines provide salient points on the elements of cyber risk management and the best practices involved.
(c)	IMO Resolution MSC.428(98), 2017[10]	It highlights the importance of Maritime Cyber Security with regard to International Safety Management (ISM) code.
(d)	The Guidelines on Cyber Security onboard ships, Baltic and International Maritime Council (BIMCO)[11]	These guidelines highlight cyber risk management framework, involvement of senior management in the process, cyber threats and vulnerabilities and regulatory compliance.

[7] **"Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems"**, International Maritime Organization, adopted on 16 June 2017.

[8] **"National Maritime Cybersecurity Plan"**, Government of United States of America, December 2020.

[9] **"Guidelines On Maritime Cyber Risk Management", MSC-FAL.1-Circ.3-Rev.2,** International Maritime Organization, 7 June 2022.

[10] **"Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems"**, no. 8.

[11] "**The Guidelines on Cyber Security Onboard Ships**" , The Baltic and International Maritime Council and International Chamber of Shipping, 9 May 2024.

(e)	US Coast Guard Cybersecurity Strategy, 2020[12]	It highlights strategic importance of cyber security, importance of protection of maritime transport system, defending and operating enterprise mission platform, integration and collaborative approach and workforce development.
(f)	UK National Strategy for Maritime Security, 2022[13]	This strategy broadly elaborates how UK will augment its capabilities in maritime cyber security amongst other verticals.

In the Indian context, the Indian Register of Shipping (IRCLASS) published Guidelines on Maritime Cyber Security in 2018. These guidelines highlight cyber risk management philosophy, cyber safety aspects like response and recovery procedures, cyber safety process review, system security controls and training/awareness.[14] Further, the Ministry of Electronics & Information Technology published Cyber Security Guidelines for Government Employees in 2022. These general guidelines focus on information security, such as internet security, mobile and e-mail security, social media security and incident reporting mechanisms.[15] It is pertinent to mention that the primary focus of the above frameworks is towards information security *with* Information Technology (IT) systems accessed by employees or maintenance representatives.

However, a focused impetus is required to address the gaps in cyber security aspects of Operational Technology (OT) and Communication Technology (CT) systems on-board merchant and naval platforms and their associated operational infrastructure at shore establishments. These systems, if compromised, can potentially lead to delayed shipments, marine accidents or even compromise entire missions in the case of naval assets. A study of maritime cyber security incidents as per type and geographical region around the world is given below.[16]

[12] **"Cyber Strategic Outlook"**, United States Coast Guard, 2021.

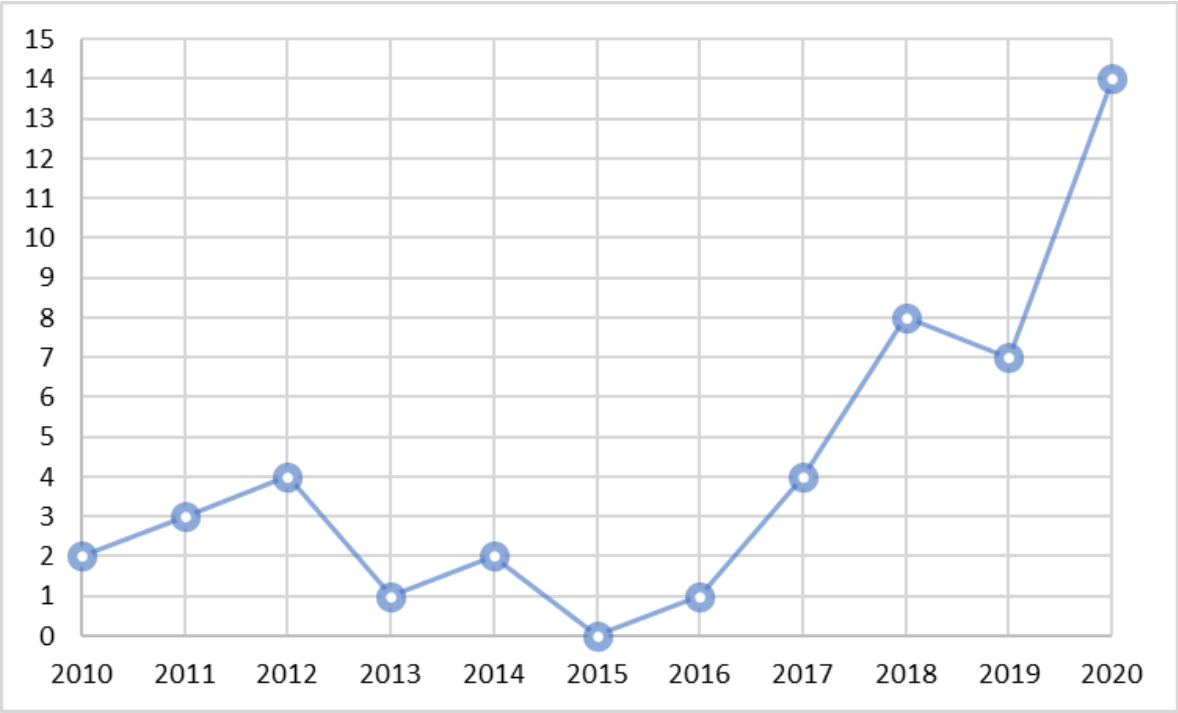
[13] **"National Strategy for Maritime Security"**, Secretary of State for Transport, United Kingdom, August 2022.

[14] **"Guidelines on Maritime Cyber Security, Revision 1"**, Indian Register for Shipping, March 2024.

[15] **"Cyber_Security_Guidelines_for_Govt_Employees, v1.4"**, Ministry of Electronics and Information Technology, Government of India, September 2022.

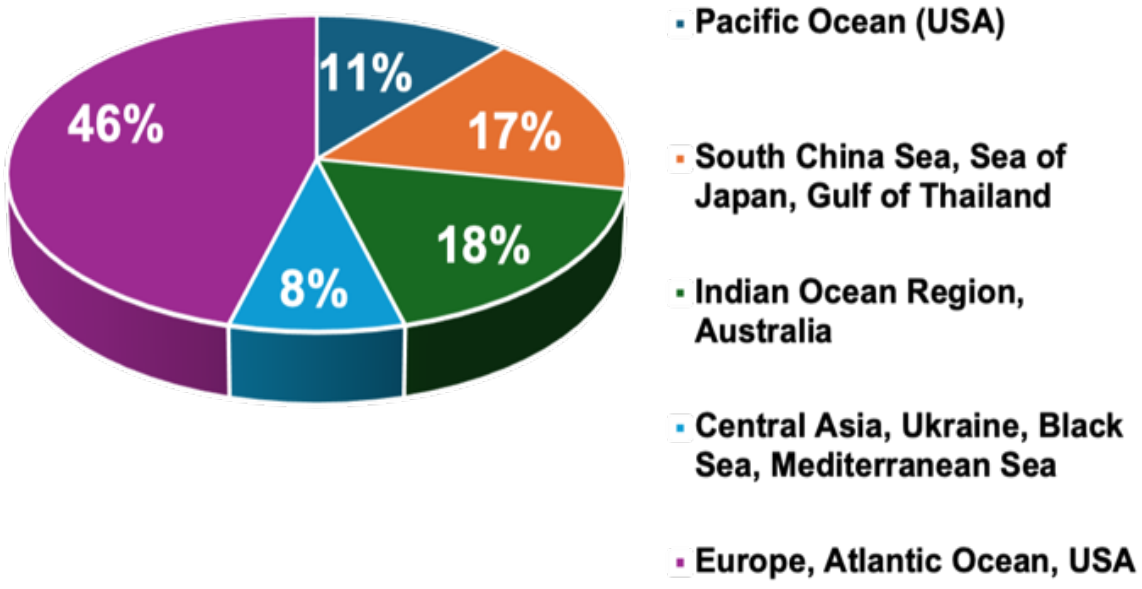
[16] **"Maritime Cyber Attack Database"**, NHL Stenden University of Applied Sciences.

Figure 3: Maritime Cyber Incidents (2010–2020)



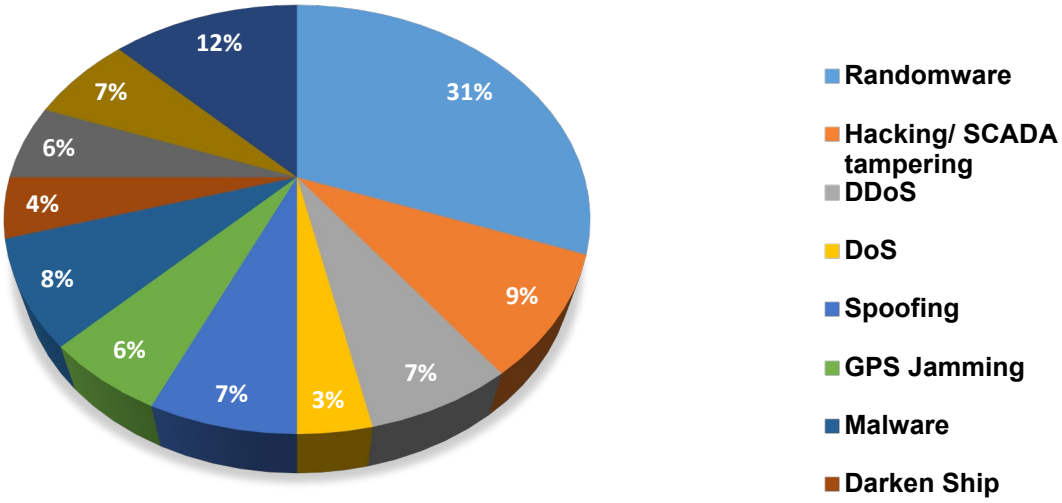
Source: P.H. Meland et al., **"A Retrospective Analysis of Maritime Cyber Security Incidents"**, *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, Vol. 15, No. 3, 2021, p. 8.

Figure 4: Maritime Cyber Incidents: Region Wise (2001–2023)



Source: https://maritimecybersecurity.nl/

Figure 5: Types of Cyber Attacks since 2001–2023



Source: https://maritimecybersecurity.nl/

India's Cyber Readiness in Maritime Domain

A cyberattack on a critical infrastructure like a nuclear power plant, an oil reserve or a power grid has the potential to cause strategic damage at the time of an imminent conflict. Hence, our response and posture need to be contemplated and suitable steps towards undertaking doctrinal changes should be undertaken. To be cyber ready, the most important aspect is to recognise cyber as a dimension of warfare akin to land, air and water. Further, it requires the availability of a dedicated and well-trained cyber force, secure systems with analytical tools, and optimum utilisation of technology for cyber defence. Further, collaboration between the military, the government, academia and private entities for adequate training of the personnel, innovation and development of cyber defence tools is critical.

Agencies like CERT, DCA and NCIIPC[17] have demonstrated strong national intent towards battling cyber threats and ensuring the cyber security of our critical assets. However, to stay at pace with the curve in maritime cyber security, the Cyber Triad—Think Cyber, Defend Cyber and Use Cyber—has to be adopted. 'Think Cyber' relates to the focus on professionals encompassing training and upgrading cyber skills and awareness to bring in a cultural change and develop informed leadership.

[17] Defence Cyber Agency (DCA) is a Tri service organisation created in 2019. CERT-IN is a national nodal agency for responding to cyber security incidents as they happen. The Government of India established the National Critical Information Infrastructure Protection Centre (NCIIPC), a division of NTRO, to support the safe, secure, and resilient information infrastructure needed by the country's critical sectors like public health, safety, energy, or national security.

'Defend Cyber' relates to identifying and mitigating the possibility of vulnerabilities in operational technologies used both in marine and naval ships like ECDIS, engine controls, firefighting and damage controls and their associated network architecture. This requires harnessing of the latest tools and technology, and generating capabilities backed with AI tools to defend own systems, networks and documentation from cyber-attacks and also to quickly recover if attacked. 'Use Cyber' relates to the need to develop and upgrade offensive capabilities such as a Cyber Operational Force at the decision level, i.e., tactical, operational and strategic.

The maritime industry is a single point of failure for global supply chains. The maritime transportation system depends on the cargo-related data stored at shore facilities and its status being monitored and, further, the performance and efficiency of the ship and the overall supply chain system being analysed at various shore-based data and analysis centres. A cyberattack on these data centres resulting in data loss or data manipulation can potentially lead to delay or failure of delivery of cargo, tampering with the cargo or even loss of cargo. Thus, safeguarding shore-based information technology assets is vital towards ensuring the cyber security of our supply chains.

Initiatives like the creation of Maritime Cyber Quick Response Teams (QRT) at each major port city for providing immediate response to a cyber threat at any maritime IT or OT asset, is essential. Usage of AI-based cyber forensics tools is equally crucial, as indeed more cohesiveness between the Shipping Corporation of India, various ports, Indian Navy, Indian Coast Guard, Army, Air Force, Paramilitary, Intelligence and other civil agencies coming under a unified ambit of a much needed, National Maritime Cyber Security Framework. This is required to develop a combined and collaborative cyber situational awareness to safeguard national economic and energy security. Further, harnessing industry talent, creating a pool of cyber experts and further utilising them in the domain of maritime cyber security will ensure sustained cyber resilience in the maritime domain for India. This will ensure that India remains abreast of the cyber curve, while concurrently serving to protect the country's maritime interests in the IOR and beyond.

In order to safeguard our maritime interests, cyber security of operational and communication technology (OT & CT) is critical. Towards that, formulation of a National Maritime Cyber Security Framework will ensure joining the resources from Indian Armed Forces, civil authorities like CERT and NCIIPC and the private sector to collaborate towards countering the ever-evolving landscape of cyber security threats in the maritime domain.

About the Author

Cdr. Adil M. Siddiqui is a serving officer in the Indian Navy.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses