ISSUE BRIEF

INSTITUTE OF STRATEGIC STUDIES ISLAMABAD
Web: www.issi.org.pk
Phone: +92-51-9204423, 24
Fax: +92-51-9204658

MARITIME CYBER-SECURITY: SECURING THE DIGITAL BACKBONE OF GLOBAL TRADE

By
Muskan Moazzam
Research Assistant
Arms Control & Disarmament Centre, ISSI
Email Address: acdc@issi.org.pk

Edited by
Malik Qasim Mustafa

July 24, 2025

(Views expressed in the brief are those of the author, and do not represent those of ISSI)

Maritime transport is the primary mode of international trade across the globe. To add to that reliance, the modern digital infrastructure has improved navigation standards, port management systems, and supply chain management. Although they have improved the efficiency of operations, the introduction of these technologies has also brought new vulnerabilities. One such vulnerability is the rising threat of cyberattacks disrupting maritime infrastructure and transportation. The infamous NotPetya[1] cyberattack on Maersk in 2017, which disrupted operations at 76 ports worldwide, is a case in point. The financial losses in that attack were estimated at a staggering amount of US$300 million[2]. In light of such threats, there are implications for countries like Pakistan because of the significance of Gwadar and Karachi ports in economic and strategic spheres within the larger CPEC framework. The elements of geopolitics and economics related to these ports add to the magnitude of threats and enhance the possibilities of disruption to these entities from potential cyber-attacks by adversaries.

The various digital systems used in modern maritime operations include the Automatic Identification System (AIS), the Electronic Chart Display and Information System (ECDIS), and cutting-edge port

1 "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," WIRED, accessed April 19, 2025, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
2 "The Untold Story of NotPetya."

© ISSI 2025 • All Rights Reserved

management software[3]. The usage of Internet of Things (IoT) and AI in smart ports has brought advanced efficiency and speed in maritime operations. The digital transformation has created an enormous new set of vulnerabilities that cyber-criminals can exploit. Ransomware and malware attacks create total paralysis in entire logistical networks. Theft of cargo manifest or ship movement data through data breaches enables criminals to conduct illegal operations, including smuggling and piracy. The manipulation of AIS data or the alteration of ECDIS systems leads vessels to make incorrect navigational choices, which results in maritime accidents and potential ship collisions. Old technologies and split-up cybersecurity standards, and a lack of worldwide regulatory standards, enhance these security challenges in maritime logistics. The International Maritime Organization (IMO) has warned that the maritime sector lags behind other industries in terms of cyber-security preparedness, with underreporting further concealing the true scale of the threat.[4]

The situation for Pakistan, therefore, becomes more critical. The Karachi port serves as the main trading hub for Pakistan, processing 60 percent of the national commerce through its digital systems yet operating without very strong cyber security protection. The smart port development of Gwadar under CPEC advanced quickly through new technology adoption but it so far lacks essential cyber-security infrastructure.[5] The efficiency-driven port modernization process makes the facility vulnerable to cyber dangers. The current high-risk geopolitical situation could render any security breach potentially dangerous because it could trigger multiple negative effects. A single attack during the 2017 NotPetya incident caused worldwide supply chains to stop functioning.[6] A cyberattack on Karachi or Gwadar would disrupt vital imports of food and energy supplies and medical products and damage investor confidence. The interconnected nature of global trade means that any security weaknesses here could trigger consequences that extend into neighboring countries.

The infusion of digital systems with AI is a double-edged sword. Therefore, various countries of the world, including Pakistan, are using AI for cyber threat detection and response. The U.S. Cybersecurity and Infrastructure Agency, for instance, uses AI for such purposes and monitors critical infrastructure networks in the country. This is because the adversaries can use AI systems to alter imaging and modify navigational information to spread false data into the systems, thereby affecting critical maritime systems. Additionally, autonomous maritime systems face enhanced threats to operational safety due to such malign interferences. Hence, the dual-edged sword of AI

3 "Maritime Cyber Risk," International Maritime Organization (IMO), accessed April 19, 2025, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.
4 "Maritime Cyber Risk."
5 Muhammad Riaz Shad, "Cyber Threat Landscape and Readiness Challenge of Pakistan," n.d.
6 "The Untold Story of NotPetya."

© ISSI 2025 • All Rights Reserved

and digital systems creates large uncertainties that can seriously affect security infrastructure and operational effectiveness.

For a solution to such problems, a range of steps can be taken. In this domain, detailed maritime cyber risk management guidelines have been issued by the IMO.[7] But, developing countries such as Pakistan suffer from inadequate application of those guidelines. The strategic value of Gwadar under CPEC requires Pakistan and China to enhance their bilateral collaboration through the exchange of cyber threat intelligence and the development of unified cyber-security standards. Additionally, blockchain technology enables data integrity through its unalterable digital record feature called block shells, which brings new potential for maritime system cyber forensics.

Public-private partnerships serve as a critical strategy to address capacity deficiencies, thus making it possible for port authorities and shipping companies to enhance security and acquire contemporary cyber-security systems. International collaboration, together with global standards compliance, allows Pakistan to acquire joint security standards and technical assistance from other nations. The development of maritime cyber-security training programs for professionals would fill any expertise gap while enabling Pakistan to handle security incidents more rapidly and efficiently.

The security of maritime systems is very important in this age. Cyber-attacks now pose a proven threat to disrupt trade and undermine the stability of the economy. Given Pakistan's dependence on its ports for both economic growth and security, it must accord higher priority to maritime cyber-security. Adversarial AI, data breaches, and mind hacking need urgent synergistic action as they present potent dangers. Pakistan needs to prepare urgently because its trade operations are becoming increasingly digital. Therefore, the implementation of AI in conjunction with block chain and psychological resilience in Pakistan's maritime cyber-security strategy is an absolute necessity. Otherwise, besides causing economic loses, it could undermine national security and serve to undercut global confidence in Pakistan's maritime capabilities.

7 "Maritime Cyber Risk."

© ISSI 2025 • All Rights Reserved