ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.02 (2026)

CYBERSECURITY IN COMMERCIAL PORTS: SAFEGUARDING OPERATIONS AGAINST EMERGING THREATS

Khatija Shahid,
M.Phil Scholar, Department of International Relations, University of Okara. Email: Khadija.shahid7631@gmail.com
Wajeeha Ghulam Ghous,
M.Phil Scholar, Department of International Relations, University of Okara. Email: wajeehachaudhary789@gmail.com
Dr. Fakhara Shahid,
Assistant Professor of International Relations, University of Okara. Email: fakhara.shahid@uo.edu.pk

Abstract:
The rapid expansion of our online world has transformed the international security environment, making digital resilience an essential aspect of national defense and economic security. Within the maritime sector, business ports have become important cyber-sensitive infrastructure due to their heavy reliance on connected virtual infrastructure. This article will examine the significance of our on-line world in marine operations and evaluate the cyber vulnerabilities of the main national industrial ports in Pakistan. The research shows a growing dependence on data technology (IT) and operational technology (OT) systems, heightening sensitivity to cyber-attacks such as ransom ware, GPS spoofing, phishing, and denial-of-carrier attacks. The paper appraises Pakistan's cyber security stance through analyzing nationwide systems, including the 2021 nationwide Cyber protection coverage, and determines the economic and defense-related impacts of cyber-attacks on naval infrastructure. The Not Petya cyber-attack is an example of case-based evaluation of global cyber incidents, using a case-based assessment of the severity of the operational and economic impacts of insufficient cyber security preparedness.
In order to address these comprehensives, this analysis proposes a comprehensive framework for hazard reduction that incorporates work for technological development, public-private partnerships, technological improvements, reforms, and international cooperation. The item concludes that strengthening cyber security resistance in business ports is not merely a technical necessity but an essential strategic imperative for safeguarding national sovereignty, maintaining trade continuity, and ensuring financial security in the virtual era.

Keywords: Maritime Cyber security, commercial Ports, Cyber Attacks, IT–OT Integration, GPS Spoofing, Port protection, countrywide Cyber security policy 2021, essential Infrastructure safety, Pakistan Maritime security, Cyber warfare, virtual Resilience

Introduction:

The digital world has completely changed how nations such as Pakistan view security, as threats and conflicts now occur online, and online security is a major component of national security. In this regard, the maritime industry, especially commercial ports, is among the most vulnerable sectors, rendering it particularly susceptible to cyber-attacks (Li, M., Zhou, J., Chattopadhyay, S., &Goh, M., 2024). This threat is also a major problem for Pakistan, with the Indian Ocean accounting for 90 per cent of Pakistan's sea trade, making major maritime centers such as Port Karachi and Port Qassim important national resources. The major vulnerability of these ports is their growing dependence on digital systems to remain efficient. There are two major types of technology utilized by modern ports, such as those in Pakistan, including Information Technology (IT) systems used for administration, logistics, billing, and communication. Operation Technology (OT) controls that operate physical equipment, including automated cranes, security sensors, navigation lights, and cargo tracking. The shift to integrated digital technologies, which is needed for modern port efficiency, means that IT and OT systems are constantly connected. Such connectivity provides numerous points of vulnerability to hackers, and this vital national infrastructure is at risk of fatal cyber-attacks

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.02 (2026)

(Lehto, M. (2022). These advanced cyber-attacks are not only about temporary computer shutdowns, but also a serious threat to national security that can harm the economy and disrupt international supply chains. With references to Port Karachi and Port Qasim, any successful cyber-attack would be disastrous; an attack carried out by a hacker would put the functioning of the port in danger, prevent the movement of ships in the contested Maritime Zones, and render the functioning of national security (Tsailas, D. N., 2025).

In 2018, MSTC was attacked, resulting in data loss and business interruptions. The cyber-attack on the Pakistan National Shipping Corporation (PNSC) in 2020 resulted in a total shutdown of the organization, demonstrating the impact on availability and business continuity. Most importantly, the 2025 Karachi Port Trust (KPT) X (formerly Twitter) social media handle hack revealed misinformation, demonstrating that ports are susceptible to confidentiality breaches (Dawn 2025, May 9).

Research shall critically examine the cyberspace environment and the vulnerabilities of the commercial ports of Karachi and Qasim. It will illuminate major cyber risks, such as GPS spoofing, ransom ware attacks, and phishing, and wrap up with suggestions of legal regulatory systems, case-based recommendations, and ethical and legal issues needed to develop a sound commercial port operations strategy (Baig, M. Z. 2025).

Research Questions:

1. What is the importance of cyberspace in the working processes of commercial ports?
2. What are the key cyber vulnerabilities of commercial ports in Pakistan, especially Karachi Port and Port Qasim?
3. What is the role of Information Technology (IT) and Operational Technology (OT) integration in improving cyber risk in port operations?
4. To what extent is the current cyber security system in Pakistan, particularly the National Cyber Security Policy 2021, effective in securing commercial ports against cyber-attacks?
5. What are the economic and defense-related impacts of cyber-attacks against commercial port infrastructure?
6. What are some legal, institutional, and technological measures to improve the cyber strength of commercial ports in Pakistan?

Research Objectives:

1. To describe the increasing role of cyberspace in the operations of contemporary commercial ports.
2. To establish and determine the top cyber risks and weaknesses of Karachi Port and Port Qasim.
3. To examine the role of IT–OT integration in increasing cyber security risks in port infrastructure.
4. To assess the policy of cyber security and the legal framework of Pakistan in protecting critical naval infrastructure.
5. To investigate the economic as well as strategic risks of cyber disruptions in port operations.
6. To provide regulatory, technical, and institutional recommendations to enhance cyber resilience at the commercial ports of Pakistan.

Research Methodology:

This research uses a qualitative, exploratory, and descriptive research methodology. The aim is to conduct an in-depth examination of the importance of cyberspace in naval operations and to evaluate the cyber vulnerabilities of major commercial ports in Pakistan, particularly Karachi Port and Port Qasim.

The study is founded mainly on secondary data. Academic articles, policy documents, government reports, cyber security studies, maritime security literature, regulatory systems, and published case studies of cyber incidents in the international maritime sector have been

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.02 (2026)

examined to gather and provide the relevant information. Particular emphasis is placed on the National Cyber Security Policy 2021 in Pakistan, international cyber security practices in maritime, and significant examples of cyber-attacks, such as the NotPetya attack and other disruptions to shipping and port systems (Melnyk, O., Drozdov, O., &Kuznichenko, S., 2025). It uses a case study approach to identify the cyber risk environment at Karachi Port and Port Qasim. Both ports are chosen for their strategic and economic significance to Pakistan's maritime trade and for their reliance on digital technology to manage cargo, communication, logistics, and support for the shipping industry. In this case-based analysis, the study determines the key weaknesses of port cyber security preparedness and institutional response capacity.

The data obtained is interpreted using a thematic analysis method. The data is categorized into key themes, such as:

- importance of cyberspace in maritime activities,
- cyber-attacks on port infrastructure,
- IT–OT integration and digital exposure,
- national cyber security governance,
- Economic and military risks,
- and regulatory and operating solutions.

The study is also analytical because it relates the current state of cyber preparedness in Pakistan to international experiences and global best practices in cybersecurity at sea. This helps develop effective recommendations to enhance cyber resilience inside commercial ports in Pakistan.

The study does not involve field surveys, interviews, or testing experiments, as it is based on secondary sources. As such, it can only find what is documented and published. Nonetheless, the approach remains applicable to policy analysis, strategic evaluation, and insight into emerging cyber security issues in the maritime sector.

Evaluating the vulnerabilities of cyberspace and changing the digital environment in Pakistan. Cyberspace in Pakistan is characterized by a vital economic infrastructure, namely the largest commercial ports of Karachi and Qasim, which handle most of the country's international trade (containerized cargo, POL products, etc.). Cargo management software, customs automation, and real-time logistics data exchanges are just a few of the interconnected digital domains that rely on an ongoing Information and Communication Technology (ICT) infrastructure to support their operations. Although this digitalization increases efficiency through workflows, such as berth scheduling and manifest processing, it creates an unconditional reliance on continuous data streams. The functional stability of Pakistan's cyberspace and, subsequently, the financial, communications, and other business sectors is therefore inherently connected to the functional stability of these two ports (Khan, M. F., Raza, A., &Naseer, N., 2021).

This cyber reliance presents a considerable, quantifiable threat, and the economic sustainability of Pakistan is at risk. The primary weakness lies in the complexity of IT/OT Integration: the merging of boundaries between Information Technology (data/software) and Operational Technology (physical equipment control). A cyber intrusion can thus quickly evolve into data theft or a physical interruption, including the suspension of terminal operations or the postponement of vessel turnaround (Ammar, M., & Khan, I. A., 2024).

The threats that exploit these vulnerabilities are intelligent and focused, such as ransom ware attacks on core port-management systems. Cargo Data Manipulation of cargo databases and logistics databases. A direct physical safety hazard is the Navigational Interference, especially the GPS spoofing of vessel navigational information. Limited cyber security maturity, use of legacy systems, and high interconnection with the global maritime network, which creates a high exposure to third-party vendors, hamper this overall cyber resilience

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.02 (2026)

(Okolo, F. C., Etukudoh, E. A., Ogunwole, O. L. U. F. U. N. M. I. L. A. Y. O., Osho, G. O., &Basiru, J. O. (2021).

The geopolitical environment elevates the threat to this infrastructure to a national security issue. The newer domain of Hybrid Warfare is in cyberspace, where enemies strive for strategic superiority. The reference to India, including cyber in its upgraded strategy, implies that the motivation behind attacks is strategic, as it seeks to render critical systems, such as financial, transportation, and military systems, ineffective.

Although Pakistan has the Prevention of Electronic Crimes Act (PECA) of 2016 in place to control sensitive data, its effectiveness is threatened. The International Telecommunication Union's assessment of cyber security places Pakistan at number 67 in the world, according to the literature (Khan, A. 2024). With such a low score, the nation's capacity to implement and maintain effective cyber defenses is far lagging behind the growing threats it is facing with strategic intent. The most critical point of the cyberspace situation in Pakistan is therefore the increasing discrepancy between the need to be digitally dependent and the development of the national cyber protection system (Khan, M. F., Raza, A., &Naseer, N., 2021). Risk assessment and vulnerabilities to Cyber to Port Karachi and Port Qasim. The digitization of the maritime supply chain presents a major vulnerability for the ports of critical Pakistan (Karachi and Qasim) to cyber-attacks. These are vulnerabilities that cross shipboard networks, AIS navigation transponders, and local port terminals. The main list of threats, as proposed by cyber security experts, is divided into three crucial categories, namely: Spoofing, Hijacking, and Disruption of System Availability (Aslan, Ö.,Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E., 2023).

The risk of AIS spoofing plus integrity attacks is significant, as the key weakness is the lack of authentication in such systems. Spoofing is the intentional relay of fake vessel positioning information that can be used to divert vessels, obscure illicit operations, or generate safety concerns to navigation due to erroneous aids. This weakens the integrity of critical navigational data, leading to operational security risks. System Hijacking and Disruption will be a direct threat to port operations and economic security. Hijacking may also take the form of ransom ware, requiring payment, or unauthorized access to transport routes and terminal operating systems. Port Control Centers can be effectively disrupted and brought to their knees through attacks such as Denial of Service (DoS) (Riskhan, B., Safuan, H. A. J., Hussain, K., Elnour, A. A. H., Abdelmaboud, A., Khan, F., &Kundi, M. (2023). These hypothetical risks are illustrated by historical events in Pakistan's maritime industry. Pakistan has already suffered severe digital security issues, indicating that the danger is imminent. This involves the high-profile breach into the Federal Board of Revenue (FBR) system that led to the disclosure of personal information. Additionally, Trojan Zed versions of trustworthy programs, such as the Pakistan Citizen Portal, have been used in the most recent cyber espionage (Khan, 2022). These incidents demonstrate that Pakistan's digital systems—including those at important ports—are constantly threatened by sophisticated threats. Finally, these cyber-attacks generate a flood of threats to Port Karachi and Qasim, bringing about the release of sensitive security information, delays in processing dangerous cargo, and the outright blockage of critical lines for national cargo and people (Nazir, T. (2024). The security of the commercial ports of Pakistan, such as Port Karachi and Qasim:

1. Inextricably linked to both economic survival and national security. The National Cyber Security Policy (NCSP) 2021 represents a significant strategic shift to safeguard such vital assets from sophisticated attacks, particularly cyber-espionage and disruption attempts, in recognition of this vital dependence. The main aim of the policy is to establish digital resilience plus develop a strong governance framework, with the Cyber Governance Policy Committee

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.02 (2026)

(CGPC) at the heart of the governance system to address the national cyber security issues (Costello, J. K., 2025).

2. In the maritime sector, the most important point of the NCSP (2021) is the defense of the Critical National Information Infrastructure (CNII). Ports are classified as Critical National Information Infrastructure (CNII), which means they must comply with national security and risk management standards. It might lead to a standoff in port operations, especially in the computerized systems that control cargo handling and port safety. The current ports are based on a combination of Information Technology (IT) and Operational Technology (OT) for crane control, security, and navigation. One of the key objectives of the NCSP (2021) is to ensure such a precarious IT/OT convergence, and the attacks, such as ransom ware or Denial of Service (DoS), that may paralyze cargo processing and shipping lines (Ammar, M., & Khan, I. A., 2024).
3. In addition, the NCSP (2021) focuses on collaboration with the business world and massive capacity building. This is a multi-agency approach essential to the maritime industry, involving the Pakistan Navy, port operators, and private logistics companies working in coordination. Pakistan is looking beyond only defence to the creation of a strong digital infrastructure that can protect the navy and the economic backbone of its commercial gateways, via training programs for port workers and the development of skills to respond to incidents rapidly and nationwide.
4. Economic and Managerial Risk Evaluation in the Disruption of Port Operations A ransom ware attack on cargo operations might have detrimental financial effects, erode investor trust, and obstruct trade. Pakistan's economy is highly vulnerable to brief disruptions since it depends on marine trade to buy energy and industrial raw materials. As Karachi and Port Qasim represent a key trade Centre, the shutdown might lead to an instant economic paralysis (Shahid, K. A. (2022).
5. A compromise of strategic impact could occur if port data discloses confidential information about CPEC logistics. The competition in the Indian Ocean, where giant powers such as the US, China, and India reside, and the cyber rivalry bring new dimensions to the regional strategic landscape. Pakistan has its vulnerabilities in cyber warfare and may be used by non-state actors and ill-intentioned intelligence services to fulfil their political interests, which may affect the stability and activity of critical infrastructure supported by China.
6. Measures to counter the threat of cyber-attacks in port operations. The development of holistic cyber security in Pakistan's critical maritime sector needs a multifaceted approach to address dangerous gaps in human resources, technology use, and international regulations. To enhance the national security posture, there needs to be an immediate increase in personnel expertise, and general simulation exercises can be used to test mission readiness Highly specialized training programs are necessary to equip navy and port personnel with the practical abilities required to identify and neutralize modern cyber-attacks, especially those that target Industrial Control Systems and Operational Technology (Oruc, A., Chowdhury, N., &Gkioulos, V., 2024).
7. At the same time, the state should deal with the systematic shortage of regulation as the number of people who rely on Information and Communication Technologies (ICT) is increasing rapidly in Pakistan, and the uneven regulation of cyberspace leaves an unprotected space, actively used by adversarial groups to undermine national security, which is manifested in targeted disinformation campaigns and advanced cyber-attacks (Akram, 2023). The presence of widespread phishing, Denial of Service (DoS/DDoS) attacks, and the spread of fake news defines this threat environment, which requires the implementation of effective technological control measures.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.02 (2026)

8. Notably, 17 out of 76 Maersk locations worldwide have had port security and logistics shut down by Petya. By using Mimi Katz and the NSA-published exploit to compromise unpatched Windows devices, the virus quickly propagated among connected networks. This vulnerability in the system also requires an immediate response to strengthen coordination among key players and implement uniform standards of cyber hygiene across both the people and the business sector. To accomplish this, effective models of public-private partnerships are required (Cheng, C. H., 2025).
9. However, international cooperation is necessary to help Pakistan address cyber risks and ensure the reliability of port data. Cooperation with technologically advanced countries, especially China, through the Digital Silk Road offers the potential to develop expertise and sophisticated defense systems to defend against cyber attacks. At the same time, the establishment of Confidence-Building Measures (CBMs) with friendly nations and an active role in international organizations, such as the IMO, can promote norms of responsible behavior in cyberspace and eliminate the danger of mistakes and exacerbation (Amin, K., Paramitha, D. I., Al Farauqi, M. D. A., &Shalehah, A., 2024).
10. Legal and Ethical aspects of cyber Incident Prevention.
11. The growing use of digital systems constitutes a significant threat due to a legal gap in international cyberspace. The existing international standards and legal regimes, including those adopted by UNCLOS, are not adequate to control complex cyber activities, leaving countries and industries highly exposed to attacks and complicating the prevention of risks (Kanwal et al., 2020). This is exacerbated by an unreliable international system in which defensive cyber operations are frequently mischaracterized as offensive operations, which may lead to economic stagnation, political anarchy, and a wider war.
12. To address these mounting problems, there is an immediate need for legally binding international agreements. Such agreements should require the adoption of common online ethics, the establishment of effective systems of accountability, protocols for interactions, and strategies for confidence-building. Of great relevance, these new frameworks ought to be able to interact with and support the current infrastructure of critical port systems smoothly, thereby guaranteeing global maritime security (Kapalidis, C., Karamperidis, S., Watson, T., &Koligiannis, G., 2022).

Case-based insights concerning Pakistan:

The Pakistan case of high-impact, systemic cyberattacks that have paralyzed global maritime giants illustrates the theoretical dangers to Pakistan's commercial ports. The analysis of these events is essential to create strong national policies towards Port Karachi and Port Qasim. The most important and topical one is the NotPetya attack in 2017, which halted operations at the world's largest shipping company, A.P. Moller-Maersk. The software, which was credited to Russian military intelligence (GRU), and targeted Ukrainian businesses, had extensive effects on supply chains around the world.

Notably, Petya has disrupted port security and logistics at 17 of 76 Maersk facilities worldwide. The malware swiftly spread among linked networks by compromising unpatched Windows devices via Mimi Katz and the NSA-published exploit. The effective spread was greatly explained by the fact that the company used rather obsolete technology and did not provide thorough network segmentation, which eventually left thousands of servers and workstations useless. The estimated financial loss to Maersk alone was up to $300 million. China Ocean Shipping Company (COSCO) experienced a cyberattack (2018); the US and Canadian operations of COSCO were the main victims of this ransomware attack. The incident caused significant disruptions to email systems and container visibility, highlighting the crucial role ransomware plays in jeopardizing confidentiality and availability in shipping logistics, even though the organization was able to isolate the impacted network and prevent a total

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.02 (2026)

system failure. The NotPetya and COSCO cases highlight the value of effective, preventive cybersecurity at Karachi Port and Port Qasim, Pakistan's main maritime commercial centers. It showed that global Operational Technology (OT) and logistics can collapse due to a deliberate assault on a single point of failure (the IT network) (Youvan, D. C., 2025).

Proposing Regulatory Mechanisms:

1. This framework provides the regulatory, technical, and human capital investments needed to achieve cyber resilience in Pakistan's key seaports, Port Karachi and Port Qasim, based on lessons learned from global events such as NotPetya. Pakistan needs to develop an elaborate cybersecurity plan specifically designed to address the ports sector. This strategy should comprise compulsory risk evaluation, established cybersecurity strategies, and straightforward, standard techniques for identifying, preventing, and responding to intrusions.

2. Found a Port Community System (PCS) as the single digital platform to eradicate paper, reduce dwell time, and link all stakeholders in real time. This will involve installing robust fiber and 5G networks and relocating administrative systems to the cloud to enhance security and flexibility.

3. Crane, Lifting, and Yard Automation, upgrade all cranes with smart sensors and DGPS to digitalize and semi-automate to gain a considerable increase in productivity and operational variance reduction. Switch to electric equipment (RMGs) where feasible to reduce fuel expenditure, reduce pollution, and shift towards more environmentally friendly, safer operations.

4. There is a compulsion to follow the rules and procedures of the International Maritime Organization (IMO). In particular, every maritime organization should focus on and apply the IMO Maritime Cyber Risk Management Guidelines to IT (Information Technology) and critical OT (Operational Technology) systems.

5. To find vulnerabilities, check compliance with international standards, and close security gaps in port management, Pakistan's government and port entities should conduct independent cyber security audits and assessments on a regular basis.

6. Support and promote public- private initiatives to invest in state-of-the-art cyber security systems and share the cost and expertise to use advanced defense systems.

7. Network segmentation is urgently needed to physically separate critical Operational Technology (OT) that controls cranes, logistics, and sensors, and typical Information Technology (IT) networks in order to prevent malware attacks and reduce the spread of malware laterally, as seen in the Not Petya attack.

8. Pakistan needs to deploy Artificial Intelligence (AI) and Machine Learning (ML) solutions to identify threats. AI-based systems should be able to monitor network activity in real time, identify suspicious activity, and anticipate network intrusions before they occur.

9. VAPT has to be performed routinely (quarterly or biannually) by ports to reduce vulnerabilities by anticipating them. It is important to regularly implement defense mechanisms, including firewalls, robust encryption, intrusion detection/prevention systems, and strict access control regulations (Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E., 2023).

10. make sure it is transparent and address the risks of third-party attacks, port management should develop the protocols to track products that are based on blockchains (where possible) and provide a deep security analysis of all third-party suppliers and vendors.

11. Pakistan needs to pay attention to developing the capabilities of the cyber workforce since they are the first line of attack. The workers at the ports need regular, compulsory training on cyber security best practices, including how to spot and report internet threats, create strong passwords, and identify phishing and social engineering tactics.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.02 (2026)

12. Develop and implement stringent measures to ensure the basics of cyber hygiene, i.e., identify and avert cyber-attacks caused by phishing emails and use of weak passwords.
13. Port Karachi and Port Qasim should be ready to act against cyber-attacks by having the complete support and help of the National Cyber Emergency Response Team (CERT) to train a workforce that can prevent and control cyber-attacks.
14.Drills and crisis simulations of high fidelity should be carried out regularly to strictly evaluate how well the reaction team works. Such drills are necessary to contain damage and recover as quickly as possible in the event of a crisis.
15. The government of Pakistan and the port authorities should prepare and ensure they have good documented Incident Response Plans to reduce the effects of cyber-attacks and to be able to recover promptly in case of any damage or disruption caused by the cyber-attack.
16. Pakistan needs to increase its digital protection by collaborating with other governments, businesses within the industry, and port authorities internationally. This is a critical partnership for intelligence sharing, harmonizing security practices, and investing in collective defense actions in the event of cyber-attacks to respond more efficiently and prevent such incidents in the future (Olakojo, K. A., & Virginia, A., 2024).

Conclusion:

Pakistan's maritime cyberspace security is a strategic need that directly affects both economic stability and national security. The shift from conventional paradigms to a robust, digitally secure ecosystem is necessary for key hubs such as Port Karachi and Port Qasim. Any inaction will carry severe repercussions, including devastating breaches of confidentiality, crippling cargo-handling delays, and safety risks due to a broken navigational aid, and can substantially cripple the movement of people and cargo across this very important trade lifeline. To reverse these mounting risks, Pakistan needs to take immediate action to change major institutional, policy, and technological policies. The essence of this change is to build a national, holistic approach to maritime cyber and to enforce compliance with international regulations, especially the IMO Maritime Cyber Risk Management Guidelines. In this strategy, a strong partnership between the public and private sectors is necessary, including civilian port authorities, shipping companies, and military cyber-defence forces.
Cyber resilience is operationally constituted by proactive efforts. To ensure compliance and preparedness, ports must implement strict policies supported by regular drills and audits. Technically speaking, it is critical to monitor network threats by installing cutting-edge technologies such as Intrusion Detection Systems (IDSs). More significantly, staff should be trained to identify and combat threats such as phishing attempts, and human capital development should be given top priority. The Navy also has to work hand in hand with the National Cyber Emergency Response Team (CERT) in training specialized units that can protect critical infrastructure in the civilian sector (Evans, C. V., Anderson, C., Baker, M., Bearse, R., Biçakci, S., Bieber, S., ... &Verner, D. (2022).
Pakistan may take a multi-layered approach to addressing the growing complexity of global cyber threats by investing in technology, human expertise, and governance. In addition to protecting its ports and improving its standing as a reliable marine partner, this kind of cooperative effort will, above all, give it economic resiliency and national sovereignty in the digital age.

References:

Li, M., Zhou, J., Chattopadhyay, S., &Goh, M. (2024). Maritime cybersecurity: A comprehensive review. *arXiv preprint arXiv:2409.11417*.

Lehto, M. (2022).Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection* (pp. 3-42). Cham: Springer International Publishing.
https://www.researchgate.net/publication/335752979_Cybersecurity_of_Critical_Infrastructure

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.02 (2026)

Tsailas, D. N. (2025). Risks And Threats In The 21st Century Maritime Security. *Security Science Journal*, *6*(1), 106-144.
https://www.securityscience.edu.rs/index.php/journal-security-science/article/view/185/121
Dawn. (2025, May 9). *KPT restores X account after hack; port operations continue as normal*. dawn.com
https://www.dawn.com/news/1909730
Baig, M. Z. (2025). Safety and sustainability in the domestic ferry sector: a PCI framework for ESG-aligned maritime governance.
https://commons.wmu.se/cgi/viewcontent.cgi?article=1041&context=phd_dissertations
Melnyk, O., Drozdov, O., &Kuznichenko, S. (2025). Cybersecurity in maritime transport: An international perspective on regulatory frameworks and countermeasures. *LexPortus*, *11*, 7.
file:///C:/Users/Tech%20Cafe/Downloads/Cybersecurity_in_Maritime_Transport_An_Internation%20(1).pdf
Khan, M. F., Raza, A., &Naseer, N. (2021). Cyber security and challenges faced by Pakistan. *Pakistan Journal of International Affairs*, *4*(4), 865-881.
file:///C:/Users/Tech%20Cafe/Downloads/11.pdf
Ammar, M., & Khan, I. A. (2024).Cyber attacks on maritime assets and their impacts on health and safety aboard: A holistic view. *arXiv preprint arXiv:2407.08406*.
file:///C:/Users/Tech%20Cafe/Downloads/11.pdf
Okolo, F. C., Etukudoh, E. A., Ogunwole, O. L. U. F. U. N. M. I. L. A. Y. O., Osho, G. O., &Basiru, J. O. (2021). Systematic review of cyber threats and resilience strategies across global supply chains and transportation networks. *Journal name missing*.
file:///C:/Users/Tech%20Cafe/Downloads/SystematicReviewofCyberThreatsandResilienceStrategiesAcrossGlobalSupplyChainsandTransportationNetworks.pdf
Khan, A. (2024).DESTINATION.
https://www.greendestinations.org/wp-content/uploads/2024/10/Top-100-2024-GPS-Chiang-Khan-From-Breakfast-Coupons-to-Chiang-Khans-Economic-Linkage.pdf
Khan, M. F., Raza, A., &Naseer, N. (2021). Cyber security and challenges faced by Pakistan. *Pakistan Journal of International Affairs*, *4*(4), 865-881.
https://www.researchgate.net/publication/361218515_CYBERSECURITY_AND_CHALLENGES_FACED_BY_PAKISTAN
Aslan, Ö.,Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.
https://www.researchgate.net/publication/369186216_A_Comprehensive_Review_of_Cyber_Security_Vulnerabilities_Threats_Attacks_and_Solutions
Riskhan, B., Safuan, H. A. J., Hussain, K., Elnour, A. A. H., Abdelmaboud, A., Khan, F., &Kundi, M. (2023). An adaptive distributed denial of service attack prevention technique in a distributed environment. *Sensors*, *23*(14), 6574.
https://www.researchgate.net/publication/372610405_An_Adaptive_Distributed_Denial_of_Service_Attack_Prevention_Technique_in_a_Distributed_Environment
Nazir, T. (2024). *Terrorist Threats To Maritime Navigation And Ports: Risk Assessment And Prevention Strategy*. Islamic Military Counter Terrorism Coalition.
https://www.imctc.org/en/eLibrary/TerrorismIssues/Documents/Terrorism%20Issues%20-%20Is%208%20-En.pdf
Costello, J. K. (2025). CYBER GOVERNANCE.
Ammar, M., & Khan, I. A. (2024).Cyber attacks on maritime assets and their impacts on health and safety aboard: A holistic view. *arXiv preprint arXiv:2407.08406*.
Shahid, K. A. (2022). Is the Physical Infrastructure in Pakistan Enough to Attract Foreign Direct Investment.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.02 (2026)

Oruc, A., Chowdhury, N., &Gkioulos, V. (2024).A modular cyber security training programme for the maritime domain. *International Journal of Information Security*, *23*(2), 1477-1512.
https://www.researchgate.net/publication/377110634_A_Modular_Cyber_Security_Training_Programme_for_the_Maritime_Domain

Cheng, C. H. (2025). *Public-private partnerships in tackling large scale cyberattacks: A comparative evaluation of the United Kingdom and Taiwan* (Doctoral dissertation, University of Southampton).
https://eprints.soton.ac.uk/505473/1/Research_V3.0_Public-Private_Partnerships_in_Tackling_Large_Scale_Cyberattacks_A_Comparative_Evaluation_of_the_United_Kingdom_and_Taiwan_PDFA-3_20250920.pdf

Amin, K., Paramitha, D. I., Al Farauqi, M. D. A., &Shalehah, A. (2024). Managing power rivalry: Indonesia's perspective and strategy in managing relations with China in the Indo-Pacific. *Dynamics in the Indo-Pacific: From geopolitics and geoeconomics perspectives*, 73-84.

Kapalidis, C., Karamperidis, S., Watson, T., &Koligiannis, G. (2022). A vulnerability centric system of systems analysis on the maritime transportation sector most valuable assets: Recommendations for port facilities and ships. *Journal of Marine Science and Engineering*, *10*(10), 1486.
https://www.mdpi.com/2077-1312/10/10/1486

Youvan, D. C. (2025). The Day the Signal Died: Systemic Collapse and Civilizational Consequences of a Global Internet Shutdown.

Aslan, Ö.,Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.
https://www.mdpi.com/2079-9292/12/6/1333

Olakojo, K. A., & Virginia, A. (2024). Strengthening cross-border cybersecurity resilience through federated threat intelligence sharing, real-time incident correlation, and coordinated governance mechanisms. *Preprint, December. https://doi. org/10.7753/IJCATR1312*, *1011*, 135.

Evans, C. V., Anderson, C., Baker, M., Bearse, R., Biçakci, S., Bieber, S., ...&Verner, D. (2022). *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)*. Centre of Excellence-Defense Against Terrorism, SSI & USAWC Press.