ISSN 3078-4220 (Print)
ISSN 3078-4239 (Online)

GLOBAL STRATEGIC PULSE

CISSS Journal of Geopolitical and Geo-Economic Studies
January - June 2025 | Volume I, Issue II

Cyberwarfare in the Maritime Domain and Strategic Stability in South Asia
Maryyum Masood, Amna Saqib, Anum A. Khan

Ripeness in the Middle East: Unpacking Iran-Saudi Arabia Rapprochement and China's New-found Role
Tayyaba Khurshid, Hassaan Malik

Understanding the Role of People's Primary Healthcare Initiative (PPHI) in Sindh
Sobia Abid

Managing the Crisis of Overpopulation in Pakistan: Need for Effective Population Management
Ajwa Hijazi

Understanding Islamophobia and Anti-Muslim Sentiment in the World
Safia Malik

Center for International Strategic Studies Sindh
CISSS
CISSS
CENTER FOR INTERNATIONAL STRATEGIC STUDIES SINDH

Cyberwarfare in the Maritime Domain and Strategic Stability in South Asia

Maryyum Masood[1], Amna Saqib[2], Anum A. Khan[3]

Abstract

The maritime domain – a global trade, communication, and national security hub – is emerging as an important theater in the evolving cyberwarfare landscape. With its increasing reliance on interconnected digital systems, this sector poses risks to commercial and military operations, with attacks capable of disrupting supply chains, compromising naval capabilities and undermining strategic security. This research examines the dual dynamics of Offensive Cyberspace Operations (OCO) and Defensive Cyberspace Operations (DCO). It focuses on their potential to escalate into full-scale cyberwarfare within the maritime sector, which may inadvertently lead to broader conflicts. Offensive operations, directed at degrading adversarial systems, and defensive operations, focused on safeguarding essential infrastructure, present challenges in managing the strategic balance. Against this backdrop, this study employs qualitative research methodology to address two key questions: (i) How can OCO and DCO lead to cyberwarfare in the maritime domain? and (ii) How can the risks of inadvertent escalation be mitigated? Through real-world case studies and an analysis of the evolving cyber capabilities of key global actors, this research highlights the vulnerabilities inherent in maritime systems and the far-reaching geopolitical risks of cyber conflicts in complex regions like South Asia, where strategic stability is essential, drawing on data obtained from primary and secondary sources. To mitigate these threats, this paper advocates for adopting a multifaceted approach: integrating advanced technological innovations such as AI-driven threat detection and quantum-resistant encryption with robust cybersecurity frameworks. It emphasizes the critical need for international collaboration, establishing explicit global norms, and confidence-building measures (CBMs) to prevent escalation and ensure stability in this key domain.

Keywords: Cybersecurity, Cyberwarfare, Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO), Strategic Stability

[1] Maryyum Masood is a Research Officer at the Center for International Strategic Studies (CISS), Islamabad.

[2] Amna Saqib is a Research Officer at the Center for International Strategic Studies (CISS), Islamabad.

[3] Anum A. Khan is an Associate Director at the Center for International Strategic Studies (CISS), Islamabad.

Introduction

The rise of cyberspace as a critical domain of modern warfare has fundamentally transformed the national security paradigms, introducing new and multifaceted challenges that transcend traditional battlefields. The maritime domain stands out as a particularly vulnerable and strategically significant frontier. Responsible for over 90% of global trade traversing the world's oceans, naval operations depend heavily on interconnected digital technologies that streamline navigation, logistics, and communication.[4] However, this increasing digitization has also introduced a host of cyber vulnerabilities, turning maritime infrastructure into a target for cyberattacks with potentially catastrophic consequences.

Cyberwarfare in the maritime domain goes beyond the traditional threats, encompassing risks to commercial shipping and naval operations. Attacks targeting ports, vessels, and interconnected digital systems can disrupt global supply chains, cause substantial financial losses and compromise national security. For naval forces, these threats are even more pronounced. Cyber intrusions into mission-critical systems, including navigation, command-and-control (C2) and weapons platforms, can paralyze fleet operations, compromise strategic capabilities and undermine readiness in contested maritime zones.[5]

The interplay of OCO and DCO further compounds the complexities of maritime cyberwarfare. OCO, designed to degrade or disrupt adversarial capabilities, have become potent tools for achieving military and political objectives, albeit with the risk of unintended escalation. Conversely, DCO are essential for safeguarding critical infrastructure and ensuring operational resilience. Striking a balance between these approaches is necessary, especially in geopolitically sensitive regions like South Asia, where the exploitation of cyber vulnerabilities could escalate into broader conflicts.[6] To examine these dynamics, this study employs a qualitative research methodology, utilizing primary and secondary sources such as academic journals, websites, and think-tank reports to analyze cyber threats in the maritime domain. This approach enables an in-depth exploration of emerging trends, strategic

[4] International Maritime Organization, *Digitalization in Shipping and Maritime Trade: Enhancing Safety and Efficiency*, https://www.imo.org/en/OurWork/MaritimeSafety/Pages/Digitalization.aspx.

[5] NATO Cooperative Cyber Defence Centre of Excellence. *Cybersecurity in Maritime Operations: Risks and Strategies for Naval and Commercial Sectors*. https://ccdcoe.org/maritime-cybersecurity.

[6] ED Lonergan and SW Lonergan, Escalation Dynamics in Cyberspace (2023), https://books.google.com/books?hl=en&id=mkOwEAAAQBAJ.

implications and potential threats in the marine domain.

This research highlights the need for robust cybersecurity measures, international collaboration and the establishment of explicit norms to address the rising tide of maritime cyber threats. Integrating advanced technologies such as Artificial Intelligence (AI), blockchain and quantum-resistant encryption can significantly enhance resilience against evolving cyber threats.

Additionally, international forums like the International Maritime Organization (IMO)[7] must lead in developing universally accepted standards for maritime cybersecurity. CBMs between adversaries, particularly in nuclearized South Asia, are crucial for preventing misinterpretation of cyber activities and maintaining strategic stability.

Cyberattacks targeting maritime operations can be broadly categorized into two types, discussed below.

Offensive Cyberspace Operations (OCO)

Offensive cyberspace operations (OCO) refer to deliberate actions within the cyberspace domain designed to disrupt, degrade, or destroy an adversary's systems, networks or data. These operations are often undertaken to achieve strategic, military, or political objectives, including undermining the capabilities of an adversary, shaping their decision-making processes or preemptively neutralizing potential threats. The primary purpose of OCO is to weaken an adversary's operational effectiveness by targeting critical infrastructure, communication networks, or defense systems. Common tactics involve deploying malware to infiltrate and control systems, exploiting zero-day vulnerabilities to access and manipulate networks and launching distributed denial-of-service (DDoS) attacks to disrupt accessibility. Other techniques, like phishing and social engineering, exploit human vulnerabilities, enabling unauthorized access or manipulating sensitive information.[8]

Several notable incidents exemplify the profound impact of OCO on global security. The 2010 Stuxnet attack,[9] allegedly carried out by the US and Israel, targeted the nuclear facilities of Iran, physically damaging centrifuges

[7] International Maritime Organization, Guidelines on Maritime Cyber Risk Management, https://www.imo.org/en/OurWork/Security/Pages/Cybersecurity.aspx.

[8] M. Libicki, "Offensive Cyber Operations and Their Place in the Theory of Coercion," Journal of Cyber Policy 5, no. 1 (2020): 5–25, https://doi.org/10.1080/23738871.2020.1728355.

[9] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014), 185–210.

and delaying its atomic program. Similarly, the 2017 NotPetya attack, attributed to Russian entities,[10] disrupted the infrastructure of Ukraine and caused collateral damage to global systems. These examples highlight the disruptive potential of OCO in achieving strategic objectives without direct physical confrontation. However, they also underscore significant legal and ethical challenges. The interconnected nature of cyberspace often results in civilian systems becoming collateral targets, raising concerns about international norms and principles of sovereignty, necessity and proportionality.[11]

OCO has emerged as a potent tool in modern conflict, enabling states to achieve objectives covertly and cost-effectively. Nevertheless, their deployment risks escalation, unintended consequences and destabilization, especially in regions where cyber capabilities have become integral to national security strategies. As the boundaries between civilian and military systems blur, the urgency for establishing explicit international norms and governance frameworks for cyberspace becomes increasingly evident.

Defensive Cyberspace Operations (DCO)

Defensive cyberspace operations (DCO) encompass a range of proactive and reactive measures designed to protect, detect and respond to cyber threats targeting digital systems, networks and data. These operations focus on safeguarding critical infrastructure, military assets and civilian networks from malicious activities, ensuring operational resilience and continuity in the face of adversarial cyberattacks. The primary goal of DCO is to uphold the integrity, confidentiality and availability of systems and information by neutralizing potential threats before they inflict significant harm.[12]

DCO can be categorized into two types: passive defense and active defense. Passive defense includes firewalls, antivirus software, encryption and access controls designed to prevent unauthorized access and mitigate known threats. Active defense, by contrast, employs dynamic approaches, such as network monitoring, threat hunting to uncover vulnerabilities and cyber forensics analysis to counter ongoing attacks. Both approaches often work in

[10] Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019), 151–176.

[11] Nils Melzer, "Cyberwarfare and International Law," IDEAS FOR PEACE AND SECURITY, 2011.

[12] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Gaithersburg, MD: NIST, 2018), https://doi.org/10.6028/NIST.CSWP.04162018.

tandem to create a robust security framework.[13]

A key aspect of DCO is its emphasis on real-time detection and rapid response. Continuous monitoring of systems helps identify threats in real-time, enabling swift responses to minimize the potential damage. For example, during a DDoS attack, DCO can include rerouting traffic, blocking malicious Internet Protocols (IPs) or using automated tools to restore system functionality. In cases of phishing attacks, DCO often involves training users to recognize deceptive emails and the implementation of email filters to block suspicious communications.

DCO are paramount to national security, particularly in protecting military systems and critical infrastructure, such as power grids, financial institutions, and transportation networks. These operations protect C2 from adversarial cyberattacks designed to disrupt military communications or compromise sensitive data. Beyond reactive measures, DCO extends to proactive strategies, including simulated cyberattack exercises, timely patching of software vulnerabilities and sharing threat intelligence across organizations and nations to enhance collective cybersecurity resilience.

In a rapidly evolving cyber environment, DCO are indispensable for mitigating risks, maintaining operational readiness and ensuring the stability of critical systems in the face of escalating cyber threats. By integrating advanced technologies such as AI, machine learning (ML) and automated threat detection, DCO continues to adapt to emerging challenges and provide a robust line of defense framework in cyberspace.

Maritime Cyberwarfare in the South Asian Context

The maritime domain, foundational to global trade, communication and security, is increasingly vulnerable to cyberwarfare. As the backbone of the worldwide economy, this sector has emerged as a prime target for cyberattacks. These attacks exploit vulnerabilities in interconnected systems and digital infrastructure to disrupt operations, exfiltrate sensitive data and assert strategic dominance. The implications extend beyond commercial shipping to naval operations, underscoring the significance of this sector as a critical focus for national and international security efforts.[14]

[13] J. Carroll, "Offensive and Defensive Cyberspace Operations Training: Are We There Yet?" in Proceedings of the European Conference on Cyber Warfare and Security, 2018, 77–88, https://books.google.com/books?hl=en&lr=&id=-kFmDwAAQBAJ.

[14] J.I. Alcaide and R.G. Llave, "Critical Infrastructures Cybersecurity and the Maritime Sector," *Transportation Research Procedia* 2020, https://www.sciencedirect.com/science/article/pii/S2352146520302209.

Modern maritime operations depend on advanced digital technologies to facilitate navigation, communication and operational management. Some systems are essential for ensuring the safe and efficient functioning of vessels. These include Global Positioning Systems (GPS), which is a navigation tool using satellites for travel; Electronic Chart Display and Information Systems (ECDIS) as an alternative to paper navigation; and Automatic Identification Systems (AIS) very high frequency (VHF) radio broadcasting to transmit and receive data between stations and ships. Similarly, ports and terminals depend on automated technologies for cargo tracking, crane operations and customs management. However, this rapid digitization and automation of these systems has introduced significant cyber vulnerabilities. Cyberattacks targeting these systems pose significant risks, including disrupting global supply chains, substantial financial losses and security threats.[15]

Modern naval forces depend equally on advanced technologies for fleet management, weapons systems and communication, making them increasingly vulnerable to cyberwarfare. Cyberattacks targeting these assets in the maritime domain exploit weaknesses in advanced digital infrastructure, posing threats to national defense. Naval operations depend on integrated fleet management, navigation and communication technologies. All services and equipment necessary for routine and survival – mission-critical operations – can be incapacitated and disrupted through cyberattacks.[16] For instance, cyberattacks on navigation systems like GPS or ECDIS could misguide naval vessels. This could result in delays, collisions or operational breakdowns that may compromise the strategic positioning of these naval vessels. Similarly, cyber intrusions into weapons systems can turn off offensive and defensive capabilities, declaring them unreliable or vulnerable to unauthorized activation. Such breaches neutralize critical assets during conflict, exposing forces to significant physical threats and strategic disadvantages.[17]

The scope of cyber threats extends beyond operational systems to encompass intelligence and command structures, where cyberattacks can exfiltrate classified information, intercept sensitive communications or inject false data.[18] Such actions compromise operational security, generate confusion and mislead decision-makers, weakening the chain of command. Adversaries

15 "Critical Infrastructures Cybersecurity and the Maritime Sector".

16 International Chamber of Shipping, The Guidelines on Cyber Security Onboard Ships, https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf.

17 KD Jones, K Tam, and M Papadaki, "Threats and Impacts in Maritime Cyber Security," *Engineering & Technology Reference* (2016),

18 Michael Schmitt, "Cyber Operations and the Jud Ad Bellum Revisited," V*illanova Law Review* (1956) 56, no. 3 (January 1, 2011): 569

with access to sensitive data, such as fleet locations or mission plans, can outmaneuver naval forces and undermine strategic initiatives. For instance, the 2017 collision of the USS John S. McCain near Singapore was speculated as a cyber-interference through naval operations targeting the ship's navigation systems. Furthermore, attacks targeting C2 systems can disrupt coordination, isolating commanders from their forces and delaying critical decisions during crises. In addition, during the 2013 alleged Iranian cyberattack, hackers could breach US naval networks and access sensitive data related to maritime operations.[19] Such vulnerabilities pose significant risks to national defense, undermining readiness and impeding timely responses to evolving threats.[20]

Several incidents highlight the growing risks of cyber intrusions, particularly among nuclear-armed states. For example, in 2017, US officials reported that Chinese cyber operatives had infiltrated the systems of a US defense contractor associated with naval operations, taking sensitive data on undersea warfare, including essential details about submarine warfare systems.[21] Such operations caused regional instability and underscored critical systems' vulnerability to sophisticated cyber intrusions. Furthermore, in 2018, Russian cyber units were accused of disrupting NATO naval exercises in the Baltic Sea by targeting communication networks, highlighting how cyber tactics can be used to challenge maritime operations in geopolitically significant waters.[22]

The broader implications of cyberattacks extend to the erosion of strategic deterrence, as adversaries exploit vulnerabilities to challenge the credibility and strength of naval forces.[23] This is especially concerning for

---

19 "Iranian Hack of US Navy Network Was More Extensive and Invasive than Previously Reported - The Verge," https://www.theverge.com/2014/2/18/5421636/us-navy-hack-by-iran-lasted-for-four-months-say-officials.

20 R.C. Wilgenbusch and A. Heisig, "Command and Control Vulnerabilities to Communications Jamming," *Joint Forces Quarterly* 69 (2013, https://ndupress.ndu.edu/portals/68/documents/jfq/jfq-69/jfq-69_56-63_wilgenbusch-heisig.pdf.

21 Office of the Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community* (2018), https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

22 NATO, *Cyber Threats to Maritime Security: Lessons from the Baltic Sea Exercises* (2019), https://www.nato.int/docu/review/articles/2019/06/01/cyber-maritime-security-lessons/index.html.

23 Kraska, J. "Maritime Power and the Cyber Domain: Securing Critical Naval Systems." Journal of Strategic Studies 42, no. 5 (2019): 685–707, https://doi.org/10.1080/01402390.2019.1567698.

nuclear-armed states, where the security of systems controlling submarines or second-strike capabilities are paramount. A breach in these systems not only jeopardizes the physical assets but also damages the psychological confidence of allies and weakens the deterrence posture against adversaries. In an era where naval power plays a pivotal role in national defense and global security, targeting military assets through cyberwarfare highlights the urgent need for robust cybersecurity measures to protect maritime operations and uphold strategic stability.

India's Advancements in Cyber Capabilities

India's advancements in cyberwarfare represent a significant development of its national security strategy, emphasizing its ambition to assert dominance in regional and global contexts. Establishing the Defense Cyber Agency (DCA) in 2018 underscores this commitment, providing India with a dedicated framework for addressing cyber threats across military domains, including the strategically critical maritime sector. Operating under the Integrated Defense Staff of the Indian Armed Forces, the DCA executes defensive and offensive cyberspace operations. Its mandate encompasses protecting India's critical military assets, conducting cyber intelligence operations and potentially disrupting adversary systems during conflict.[24] India has opted for military units such as Command Cyber Operations and Support Wings (CCOSWs) for cyber defense to facilitate its joint forces. India has also formulated a new joint doctrine for cyberspace operations to integrate the Army, Air Force and Navy.[25]

One of the key focuses of India's cyber strategy is the maritime domain, reflecting its importance to the country's geopolitical and economic goals. The Indian Navy, as the foundation of India's naval power, has systematically integrated cyber capabilities into its operations to safeguard critical assets such as maritime fleets, communication networks and infrastructure in strategically essential locations such as the Indian Ocean Region (IOR).[26] This integration strengthens the ability of the Navy to counter cyberattacks targeting navigation systems, C2 networks and logistics frameworks while also enabling it to

[24] Indian Ministry of Defence, Defence Cyber Agency: A Strategic Initiative, 2018, https://mod.gov.in/defence-cyber-agency-overview.

[25] "Armed Forces Formulate New Doctrine for Cyberspace Operations," *The Times of India*, June 18, 2024, https://timesofindia.indiatimes.com/india/armed-forces-formulate-new-doctrine-for-cyberspace-operations/articleshow/111089679.cms.

[26] David Brewster, "Cybersecurity and the Indian Ocean: Challenges and Opportunities,"*Journal of Indian Ocean Studies* 29, no. 2 (2020): 45–62. https://indianoceanstudiesjournal.org/cybersecurity-indian-ocean.

conduct preemptive cyber offenses if required.[27]

India's collaboration with technologically advanced countries such as the US and Israel has strengthened its cyber capabilities. Partnerships with these countries have provided India access to cutting-edge technologies, joint training programs and intelligence-sharing frameworks. For example, the Indo-US Cyber Framework Agreement[28] facilitates cooperation on cybersecurity and cybercrime, enhancing India's ability to counter threats and develop offensive capabilities. Similarly, India's partnership with Israel[29] includes joint research and development in cyber technologies. This has enabled adopting advanced tools and techniques for cyber defense and warfare.

These collaborations have significantly enhanced India's ability to conduct cyber espionage and cyberattacks, particularly in sensitive domains like maritime security. By leveraging these partnerships, India has reportedly developed advanced cyber capabilities to target critical infrastructure and defense systems in adversarial states. Cyber groups linked to India have been implicated in espionage campaigns targeting Pakistani government and military systems, including operations aimed at gathering intelligence on military and nuclear systems.[30] While specific publicly disclosed instances of Indian cyberattacks targeting Pakistan's maritime C2 systems are limited, there have been reports suggesting that India has engaged in cyber espionage activities targeting the marine assets of Pakistan. Notably, the Indian-linked cyber espionage group known as SideWinder has expanded its operations to target maritime facilities, including those in Pakistan.[31] This group has been observed conducting spear-phishing attacks using falsified documents from specific ports to compromise systems and networks at naval facilities. Such capabilities position India to assert strategic influence through cyber means, particularly in regions like the Arabian Sea and the Indian Ocean.

---

27 Pravin Sawhney, "India's Cyber Warfare Capabilities and Regional Implications," *Strategic Analysis* 45, no. 4 (2021): 360–375, https://doi.org/10.1080/09700161.2021.1940025.

28 Indian Ministry of External Affairs, *Indo-US Cyber Framework Agreement*, 2016, https://mea.gov.in/indo-us-cyber-framework.pdf.

29 Amir Rapaport, "India-Israel Cyber Partnership: A Growing Alliance," *Cybertech Quarterly*, no. 3 (2020): 18–25, https://cybertechquarterly.com/india-israel-cyber-partnership.

30 "Suspected Nation-State Adversary Targets Pakistan Navy in Cyber Espionage Campaign," https://blogs.blackberry.com/en/2024/11/suspected-nation-state-adversary-targets-pakistan-navy-in-cyber-espionage-campaign.

31 S. Checkley, "SideWinder: An Indian Espionage Group Targets Maritime Infrastructure," *Cybersecurity Quarterly*, 2021, https://cybersecurityquarterly.com/sidewinder-report.

Indian investments in cyberwarfare capabilities, mainly through initiatives like the DCA and international collaboration, signal its intent to dominate cyberspace as a cornerstone of its national security architecture. However, these advancements also contribute to regional cyber instability. Pakistan views India's growing cyber expertise as a direct threat to its critical infrastructure and defense systems, particularly in the maritime domain.[32] This escalating dynamic underlines the urgent need for regional dialogue on cyber norms to mitigate risks, prevent escalation and maintain stability in South Asia.[33]

Pakistan's Cybersecurity Posture

Pakistan's cybersecurity posture has evolved significantly in recent years as it seeks to address the growing threat of cyberattacks, particularly in sensitive domains like maritime operations. Recognizing the strategic vulnerabilities posed by evolving cyber threats,[34] Pakistan has undertaken significant efforts to strengthen its cybersecurity infrastructure, focusing on developing defensive and offensive capabilities to protect its critical assets and maintain strategic stability in the region.

Pakistan's vulnerabilities are particularly pronounced in the maritime domain due to its reliance on key naval assets and infrastructure, including Karachi Port, Gwadar Port and interconnected logistics networks. These facilities are vital for Pakistan's economic sustainability, including the China-Pakistan Economic Corridor (CPEC) and its national security. The Pakistan Navy plays a critical role in defending these assets and ensuring freedom of navigation in the Arabian Sea, a region with significant strategic importance due to its proximity to the Strait of Hormuz and the Indian Ocean. However, the increasing digitization within naval systems, including navigation and C2 networks, has introduced new vulnerabilities.[35] These digital dependencies create potential exploitation opportunities for adversaries, particularly India.

---

[32] Ministry of Foreign Affairs Pakistan, December 10, 2020, https://mofa.gov.pk/transcript-of-the-press-briefing-by-spokesperson-on-thursday-10-december-2020.

[33] Sanjana Varghese, "Cybersecurity in South Asia: Strategic Implications of India's Cyber Capabilities," Asian Security 17, no. 2 (2021): 130–145, https://doi.org/10.1080/14799855.2021.1890103.

[34] Nighat Dad, "Evolving Cybersecurity in Pakistan: Strategies and Challenges," *Journal of Strategic Cyber Studies* 8, no. 3 (2022): 75–92, https://doi.org/10.1080/20474125.2022.1980842.

[35] Pakistan Navy, *Strategic Cybersecurity Framework for Maritime Defense*, 2023, https://www.paknavy.gov.pk/cybersecurity-policy.

Pakistan has taken several measures to strengthen its cybersecurity posture in response to escalating cyber threats. Adopting the National Cyber Security Policy and establishing cyber command capabilities within the armed forces reflect Pakistan's clear commitment to addressing cyber threats. The 2021 National Cyber Security Policy[36] provides a comprehensive framework for safeguarding critical infrastructure, enhancing cyber resilience and equipping national institutions to respond to cyber threats effectively. It emphasizes establishing governance and institutional mechanisms to protect national information systems and ICT infrastructures through monitoring, detection, protection and response strategies. In the maritime sector, specific efforts focus on integrating robust cybersecurity measures into naval operations, including securing digital systems aboard vessels, protecting C2 structures and leveraging AI and real-time monitoring for threat detection and response. The policy also underscores the importance of public-private partnerships and collaborative mechanisms to strengthen cybersecurity capabilities through technical and operational cooperation. Additionally, it highlights the need for capacity building, skill development and training programs to cultivate a skilled cybersecurity workforce. Furthermore, the policy advocates for a national-global cooperation framework to effectively address evolving cybersecurity challenges.

Pakistan has also been advancing its offensive cyber capabilities as part of its broader strategy to deter and counter cyber threats. These capabilities enable Pakistan to respond to cyber intrusions and protect against potential threats targeting its maritime assets. For example, cyber threat intelligence gathering and the ability to disrupt adversarial networks have become central to ensuring the security of naval operations in Pakistan. Moreover, Pakistan has benefited from international partnerships, particularly with China, to increase its cyber defense capabilities. China's experience in cyberspace and its collaboration with Pakistan under the CPEC framework have significantly supported Pakistan's efforts to secure its critical maritime infrastructure and strengthen its overall cybersecurity landscape.

Pakistan's emphasis on cybersecurity in the maritime domain reflects its broader strategic priorities, particularly in response to India's growing cyber capabilities. India's advancements through the DCA and partnerships with the US and Israel are perceived by Pakistan as a direct threat to its national security. Indian-linked cyber groups targeting Pakistani government and military systems, including those within the maritime sector, have further highlighted the urgency of enhancing the cyber defenses of Pakistan. Such Indian

[36] Pakistan Ministry of IT and Telecommunication, National Cyber Security Policy 2021, https://moitt.gov.pk/national-cyber-security-policy.

advancements in cyberspace are viewed not only as a challenge to Pakistan's operational security but also as a potential avenue for escalating regional tensions. While Pakistan has made significant progress, the dynamic nature of cyber threats necessitates continuous investment in advanced technology, workforce training and international partnerships to maintain long-term resilience and regional stability.

Potential for Escalation between India and Pakistan in the Maritime Domain

The risk of escalation in the maritime domain between India and Pakistan, driven by cyber vulnerabilities, is a critical concern given the geopolitical tensions and the strategic importance of their naval operations. Both states increasingly depend on digital systems to manage maritime navigation, communication and operations, making these systems prime targets for cyberattacks. The interconnected nature of maritime networks amplifies the risks, as even a localized cyber incident could have far-reaching effects on regional stability, impacting the targeted states and broader geopolitical dynamics.

Offensive cyber operations, particularly those aimed at naval C2 systems, present a hazardous scenario. These systems are crucial for coordinating fleet movements, managing weapons systems and maintaining situational awareness at sea. A successful infiltration or disruption of C2 systems could paralyze naval operations, leaving ships and submarines vulnerable to physical threats or operational breakdowns. Such an attack could also trigger an intense retaliatory action, especially perceived as a calculated act of aggression, further increasing the risk of conflict escalation in the region.

A cyberattack targeting navigation systems like GPS or ECDIS could have equally destabilizing consequences. For example, if the navigation system of a naval vessel were compromised, the ship might inadvertently enter restricted or disputed waters, potentially breaching territorial boundaries. In India and Pakistan, where maritime boundary disputes remain contentious and tensions over maritime boundaries remain high, such an incident could rapidly escalate into a military confrontation. For instance, following the Balakot crisis in 2019, the Pakistan Navy successfully intercepted and prevented an Indian submarine from entering Pakistani waters. This incident highlighted the heightened tensions between the two countries and underscored the

significance of maritime security in maintaining regional stability.[37] In this context, a cyber-induced navigational error or such an attempt during a crisis might be misinterpreted as an intentional act of aggression, prompting an immediate and potentially disproportionate retaliatory response.

Cyber operations targeting maritime traffic management systems in ports and coastal waters pose additional risks with far-reaching implications. Disrupting these systems could lead to vessel collisions, grounding of vessels or blockages in critical sea lanes, impacting military operations and global commercial shipping. The strategic significance of Pakistan's Gwadar Port and India's ports along the western coastline amplify the stakes, as any disruption in maritime traffic could be perceived as a deliberate effort to undermine its economic stability or diminish its geopolitical influence, further fueling tensions.

Historical incidents highlight the risks of cyber operations in geopolitically contested regions. In 2017, reports of GPS spoofing in the Black Sea, attributed to geopolitical tensions, highlighted the potential of cyber tactics to mislead maritime navigation systems. When applied to the India-Pakistan context, where India possesses advanced offensive cyber capabilities, the likelihood of escalation through such tactics is significantly heightened. Even unintended or misattributed cyber incidents could rapidly escalate into broader conflicts, as the speed and lack of transparency inherent to cyber operations often leave little room for diplomatic resolution before retaliatory actions are initiated.

The absence of established international norms governing cyber activities in the maritime domain further exacerbate these risks. Without clearly defined rules of engagement, actions taken under the guise of defensive measures or cyber reconnaissance could be misinterpreted as offensive provocations, further destabilizing the region. This highlights the urgent need for naval CBMs, transparency and sustained dialogue between India and Pakistan to prevent cyber incidents from escalating into broader maritime or military conflicts.

[37] Ali Osman, "Navy Thwarts Attempt by Indian Submarine to Enter Pakistani Waters," The Express Tribune, March 5, 2019, https://tribune.com.pk/story/1923388/navy-thwarts-attempt-indian-submarine-enter-pakistani-waters.

Mitigating the Risks

Addressing the risks of cyberwarfare in the maritime domain for Pakistan requires a comprehensive and multidimensional approach to address vulnerabilities, enhance defensive capabilities and promote regional and international cooperation. Strengthening the cybersecurity infrastructure of critical maritime systems, including navigation, communication and operations platforms like GPS and AIS, is a foundational step. Moreover, implementing advanced firewalls, encryption protocols and multi-layered defenses can substantially reduce the likelihood of unauthorized intrusions. Additionally, segregating critical military systems from civilian networks and conducting regular vulnerability assessments may help identify and address potential security gaps. Equally important is the advancement of both defensive and offensive cyber capabilities to ensure resilience and strengthen deterrence posture. Real-time threat detection and response, powered by AI and ML, can enhance Pakistan's ability to detect and respond to cyber threats. Simultaneously, offensive cyber capabilities can serve as a deterrent, signaling the capacity to neutralize adversarial threats. This two-pronged approach, integrating proactive defense with strategic offense, is essential for safeguarding Pakistan's maritime assets and ensuring operational readiness in a rapidly evolving cyber landscape.

Enhancing cybersecurity in Pakistan's maritime domain requires an increased focus on training and awareness among naval personnel.[38] Specialized training programs can equip naval and port staff with the necessary skills to identify and mitigate cyber risks, while simulation exercises can evaluate response protocols and strengthen operational readiness. Securing ports like Gwadar and Karachi also requires implementing robust cybersecurity measures, including advanced intrusion detection systems and technologies like blockchain, to protect the integrity and reliability of maritime data. International collaboration is vital in increasing Pakistan's capacity to counter cyber threats. Partnerships with technologically advanced states, such as China, can provide access to technical expertise and support in developing advanced cyber defense systems. Simultaneously, initiating naval CBMs with India and actively participating in international forums like the IMO can promote norms of responsible behavior in cyberspace, reducing the potential for miscalculations.[39]

[38] S.M. Shahzad, "Strengthening Maritime Cybersecurity: Training and Technological Solutions," *Journal of Maritime Security Studies* 14, no. 2 (2023): 98–115, https://doi.org/10.1080/20474125.2023.3091721.

[39] L. Zhou, "Collaborative Cybersecurity Strategies between Pakistan and China," *South Asia Cybersecurity Quarterly* 16, no. 3 (2022): 56–72, https://doi.org/10.1080/20474120.2022.3067893.

Technological innovation is key in mitigating cyber risk in Pakistan's maritime domain. Leveraging AI-driven threat detection systems and adopting blockchain technology for secure data management can significantly enhance the cybersecurity of naval operations. Investing in advanced technologies such as quantum-resistant encryption may help foolproof Pakistan's cybersecurity framework against emerging and sophisticated threats. Furthermore, establishing incident response teams dedicated to maritime cybersecurity would enable rapid recovery from attacks, minimizing operational disruption and economic impact. At the policy level, integrating cybersecurity into national frameworks, such as the National Cyber Security Policy, ensures sustained focus, resource allocation and strategic alignment in this vital sector.

Public and governmental awareness can also be raised to emphasize the importance of cybersecurity in the maritime sector. Awareness campaigns targeted at stakeholders, including shipping companies and logistics providers, can enhance collective resilience. By combining advanced technologies, international cooperation, strategic policy frameworks and a well-trained workforce, Pakistan can build a robust maritime cybersecurity framework. These efforts are essential to safeguarding critical maritime assets, maintaining operational continuity and maintaining regional stability in the face of evolving cyber threats.

Legal and Ethical Frameworks in Maritime Cyberwarfare

The maritime domain's growing dependence on interconnected digital systems has introduced unique vulnerabilities, making it a critical target for cyber operations. However, the lack of explicit international norms and legal frameworks to regulate cyber activities in this domain exacerbates the risks of conflict escalation and miscalculation. While existing conventions, like the United Nations Convention on the Law of the Sea (UNCLOS), offer a framework for maritime governance, they are insufficient to address the multifaceted challenges posed by cyber threats. This regulatory gap leaves countries and industries operating in a legal and ethical vacuum, complicating efforts to manage and mitigate cyber risks.

The strategic significance of the maritime domain to global trade and security heightens the urgency of this issue. Cyberattacks targeting navigation systems, port infrastructure or naval assets could trigger severe consequences, including economic disruption, geopolitical instability, and inadvertent escalation into broader conflicts. Without established international norms, defensive actions may be misinterpreted as offensive provocations, increasing the potential for retaliatory measures and further destabilizing a fragile,

substantial escalation.

To address these challenges, the development of binding international agreements is essential. Such contracts should define acceptable behavior, establish accountability mechanisms and promote ethical standards in cyberspace. Key elements of these frameworks could include:

1. Rules of Engagement: Clear definitions of what constitutes a cyberattack, permissible defensive measures and proportional responses to mitigate the risks of escalation.
2. Transparency and Confidence-Building Measures: Mechanisms for sharing information about cyber threats and incidents to promote trust among countries and reduce the likelihood of misattributed attacks.
3. Accountability Mechanisms: Processes to hold state and non-state actors accountable for cyberattacks, ensuring that perpetrators face consequences under international law.
4. Integration with Existing Maritime Frameworks: Updating conventions like UNCLOS to incorporate cyber-specific clauses, aligning traditional maritime governance with modern challenges.

The IMO is well-positioned to lead these efforts to address cybersecurity challenges in the maritime sector, given its mandate to ensure marine safety and security. Collaborative initiatives involving the IMO,[40] UN and regional organizations could establish globally recognized norms governing cyber operations in the maritime sector. For instance, the IMO's existing maritime cyber risk management guidelines could be expanded into a comprehensive regulatory framework that addresses the broader implications of cyberwarfare and its impact on global security. Ethical considerations should form a core component of these frameworks.

Regarding CBMs and other risk reduction measures at sea, multiple proposals could be considered by both India and Pakistan to mitigate the risks of cyberspace incidents in the naval domain escalating into conflict. For instance, establishing a data-sharing mechanism and mutual notifications regarding cybersecurity threats could significantly reduce misunderstandings and enhance trust. This is particularly important given both states' increasing reliance on the maritime domain's digitalization. Additionally, Pakistan and India could expand their existing CBM on non-attack agreements concerning

[40] Ramesh Thakur, "The Role of the UN and IMO in Establishing Cyber Norms," *South Asia Strategic Review* 20, no. 3 (2023): 91–108, https://doi.org/10.1080/15423174.2023.3118462.

nuclear facilities to include commitments in the cyber domain, specifically prohibiting cyberattacks on nuclear facilities.

By addressing these legal and ethical challenges, states can create a stable and predictable environment for maritime operations, thereby reducing the risks of cyber conflicts. Establishing such regulatory and ethical frameworks is not merely a procedural requirement but a strategic imperative to protect the maritime domain in an era of increasing digitization and cyber vulnerabilities.

Conclusion

As a cornerstone of global trade and national defense, the maritime domain has become a critical battleground in the escalating landscape of cyberwarfare. The increasing dependence on interconnected digital systems for navigation, logistics, communication and defense has exposed significant vulnerabilities, making commercial and military operations susceptible to cyberattacks. These threats jeopardize operational continuity and pose broader regional and global security risks, particularly in geopolitically sensitive regions like South Asia.

OCO have demonstrated the capability to effectively disrupt adversarial systems, enabling strategic objectives without traditional military engagement. However, these operations carry substantial risks, including escalation, miscalculation and unintended consequences, especially in contested maritime boundaries and during high-stakes naval confrontations. In contrast, DCO are indispensable for protecting critical infrastructure, ensuring resilience and maintaining strategic deterrence. The dynamic interplay between OCO and DCO highlights the importance of a balanced, proactive cybersecurity strategy to protect the maritime sector from evolving threats.

Addressing these complex challenges of maritime cybersecurity requires a comprehensive strategy that integrates robust cybersecurity mechanisms, technological innovation, workforce training and international collaboration. In regions like South Asia, where geopolitical tensions between India and Pakistan remain high, the potential for cyber incidents in the naval domain to escalate into broader conflicts is particularly concerning. Historical examples and advancements in offensive cyber capabilities highlight the urgency of addressing these risks through robust cybersecurity frameworks, advanced technological integration and mutually agreed CBMs. Establishing mechanisms such as data-sharing and non-attack agreements on nuclear

facilities within the cyber domain could play a pivotal role in reducing misunderstandings and preventing escalation.

Furthermore, international collaboration and the development of comprehensive legal and ethical frameworks are essential to mitigate risks and ensure the stability of global maritime operations. Organizations like the IMO can lead efforts to create universally accepted cybersecurity standards, aligning them with existing maritime governance frameworks. For Pakistan, strengthening its defensive and offensive cyber capabilities, enhancing training programs and fostering international partnerships will be key to safeguarding its naval assets.

In sum, the increasing prominence of cyberwarfare within the maritime domain is a stark reminder of the urgent need to prioritize cybersecurity in this vital sector. As the boundaries between physical and cyber domains blur, protecting maritime operations from cyber threats has evolved from a technical challenge to a strategic necessity. By promoting international collaboration, advancing technological defenses and developing explicit international norms, the global community can collectively work toward ensuring the stability and security of the maritime domain in an era of unprecedented connectivity and digital interdependence.