ISSUE 18 / JANUARY 2026

BLUE SECURITY

A MARITIME AFFAIRS SERIES

Ensuring Cybersecurity in Ports for Major Port States in Southeast Asia

Su Wai Mon and Vu Hai Dang

BLUE SECURITY
THE UNIVERSITY OF WESTERN AUSTRALIA
UWA DEFENCE & SECURITY
UNITED STATES STUDIES CENTRE
UNSW CANBERRA
AP4D Asia-Pacific Development, Diplomacy & Defence Dialogue
LA TROBE UNIVERSITY

BLUE SECURITY

The Blue Security Program engages with and facilitates high quality research on issues of critical maritime security across the Indo-Pacific. Bringing together leading regional experts in politics, international law and strategic studies, Blue Security focuses on three key pillars of maritime security: order, law and power.

Blue Security is a collaboration between La Trobe Asia, University of New South Wales Canberra (ADFA), University of Western Australia's Defence and Security Institute (DSI), United States Studies Centre at the University of Sydney (USSC) and the Asia-Pacific Development, Diplomacy & Defence Dialogue (AP4D).

It produces working papers, commentaries, and scholarly publications related to maritime security for audiences across the Indo-Pacific.

The Blue Security consortium is led by Professor Rebecca Strating (La Trobe Asia, La Trobe University), Professor Douglas Guilfoyle (UNSW Canberra), Professor Peter Dean (United States Studies Centre), and Melissa Conley Tyler (Asia- Pacific Development, Diplomacy & Defence Dialogue).

Dr Troy Lee-Brown (Defence and Security Institute, University of Western Australia) is the Project Manager.

Blue Security receives funding support from the Department of Foreign Affairs and Trade, Australia.

Views expressed are solely of its author/s and not representative of the Maritime Exchange, the Australian Government, or any collaboration partner country government.

Please direct inquiries to troy.lee-brown@uwa.edu.au

bluesecprogram
blue-security-program
bluesecprogram.bsky.social
BlueSecProgram

MARITIME AFFAIRS SERIES EDITORS

Professor Bec Strating

Bec Strating is the Director of La Trobe Asia and a Professor of Politics and International Relations at La Trobe University, Melbourne. Her research focuses on maritime disputes in Asia and Australian foreign and defence policy. She has an extensive track record in writing research publications including three monographs, most recently "Defending the Maritime Rules- Based Order" (2020). She is currently a non-visiting fellow at the Royal Australian Navy's Seapower Centre, a member of the East West Centre Council on Indo-Pacific Relations, and chair of the Women in International Security Australia's steering committee. Bec serves on the editorial boards of the Australian Journal of International Affairs and Journal of Maritime and Territorial Studies.

Dr Troy-Lee Brown

Troy Lee-Brown is a researcher in regional security, maritime security and international relations with a focus on defence and security issues in the Indo-Pacific. He is currently a Research Fellow at the Defence and Security Institute at the University of Western Australia and is also the Program Manager for the Blue Security Program a DFAT funded project which focuses on issues of maritime security in the Indo-Pacific. Troy is the editor of the DSI Black Swan Strategy Paper and also Blue Security: A Maritime Affairs Series. His research interests include maritime security, defence and security policy, with a focus on the Indian Ocean and broader Indo-Pacific.

MARITIME AFFAIRS SERIES AUTHORS

Dr. Su Wai Mon

Dr. Su Wai Mon is a Research Fellow in Oceans Law and Policy at the Centre for International Law (CIL), National University of Singapore. She holds a PhD in maritime security and law enforcement and is currently a Blue Security Fellow with the La Trobe Asia Blue Security Programme (La Trobe University, Australia).

Previously, Su served as a Senior Lecturer at the Faculty of Law, University of Malaya (UM) and she led research projects funded by the Malaysia's Ministry of Higher Education, focusing on maritime cybersecurity and the protection of submarine communication cables. Under the national grant, she organized domestic and international workshops on maritime cybersecurity, in collaboration with the Defence Cyber and Electromagnetic Division of the Malaysian Armed Forces.

Su participated in the IMO Cyber-SHIP Lab Symposium in London (2024) and has presented on maritime cybersecurity at multiple conferences and workshops, including the 2025 International Maritime Security Conference hosted by the NATO Maritime Security Centre of Excellence (MARSEC COE), the NATO MARSEC COE Maritime Situational Awareness Working Group Meeting, and the ASEAN Maritime Cybersecurity Conference co-hosted by the Ministry of Defence Malaysia and the Australian Department of Defence.

Her research focuses on emerging technologies and maritime security, the law of the sea, maritime cybersecurity and submarine cable governance. She is committed to fostering interdisciplinary and cross-sector collaboration to address emerging challenges in critical maritime infrastructure and security governance.

Dr. Vu Hai Dang

Dr. Vu Hai Dang is Acting Director of Maritime Diplomacy Centre at the Diplomatic Academy of Viet Nam. His area of expertise includes international law, law of the sea, and international environmental law with a geographical focus on Southeast Asia and the South China Sea. He has experience working in the fields of private practice, civil service, diplomacy, and academia.

Dr. Vu Hai Dang's latest publications include *Quiet Diplomacy under Anwar Ibrahim Administration: Implications for Malaysia's South China Sea Strategy and Regional Security,* June 2025 (journal article in International Studies Review); *ASEAN: Important Broker for Marine Scientific Research Cooperation in the South China Sea Asia,* 2025 (book chapter), and *UNCLOS 30 Years' Implementation: An Assessment, 2025* (edited book with Springer), and *Viability of UNCLOS amid Emerging Global Maritime Challenges,* 2024 (edited book with Springer).

CONTENTS

ABSTRACT

Maritime ports play a pivotal role in the global economy, handling billions of tonnes of cargo annually. The security landscape of ports has evolved alongside their modernisation, which increasingly integrates technologies such as Information Technology (IT), Operational Technology (OT), Internet of Things (IoT), cloud computing, and digital data management. This growing digitalisation has, however, exposed ports to a rising number of cyber threats, as seen in recent incidents including the Port of Nagoya cyber attack, the DP World Australia incident, and Port of Seattle cyber attack. Cybersecurity now ranks among the top risks for ports, alongside piracy and terrorism, yet many ports remain underprepared. Every device, software, and network connection must be secured due to the highly complex and interconnected nature of port systems. According to a report by Lloyd's of London, a single cyber attack on major ports in the Asia-Pacific could result in losses of up to US$110 billion.

Southeast Asia hosts some of the world's busiest ports, including the Port of Singapore, Port of Tanjung Pelepas, and Belawan Port in Indonesia, all located along or near the Strait of Malacca, one of the busiest and most critical maritime chokepoints globally. Disruptions to these hubs would have severe consequences for the global maritime supply chain. While ports in the region are adopting advanced technologies to enhance efficiency and capacity, accelerating digitalisation also increases vulnerability to cyber threats. The diverse management structures and multiple operators across ports, combined with the absence of uniform security standards, exacerbate these vulnerabilities.

Given these challenges, there is a pressing need for systematic, harmonized regulatory frameworks and compliance mechanisms to strengthen port cybersecurity across Southeast Asia. Ensuring cyber resilience requires coordination between public authorities, private operators, and international standards. This paper seeks to provide recommendations for regulatory and policy readiness in major Southeast Asian ports, aiming to address cybersecurity gaps, improve preparedness, and safeguard the region's critical maritime infrastructure.

Keywords: *maritime security, port security, cybersecurity, Southeast Asia, critical maritime infrastructure*

PORT SECURITY IN THE 21ST CENTURY: THE OVERVIEW

It is reported that about 90 % of all global trade flows through just 39 bottleneck regions in the world.[1] In the future, global trade will increase along these so-called crucial choke points of the supply chain, and the geographic location where there is only one narrow waterway are significant weak points. Any disruptions against the safety of navigation through them would have major implications for the global supply chain – such as the Ever Given blockage in the Suez Canal, which caused a backlog of some 400 stranded ships, and an estimated loss to the global economy of USD $ 400 million for every hour the shipping was stuck.[2] In recent years, cyber attacks on ports have made headlines, including Jawaharlal Nehru Port Terminal attack in 2022[3], Japan's Nagoya Port ransomware attack 2023,[4] and the Port of Seattle cyber attack in 2024.[5] Such attacks highlight the vulnerabilities of critical maritime infrastructure in the global maritime supply chain. Major ports of Southeast Asia, strategically positioned along the Straits of Malacca, are vital corridors connecting Europe and the Middle East to East Asia. Ensuring the cyber resilience of these ports is crucial, along with fostering cooperation among key port nations such as Singapore, Indonesia, and Malaysia.

The security of maritime ports is vital to the global economy.[6] In the policy context, ports are now viewed as essential 'nodes' within the supply chain, with port-related policies shaped by the broader demands of global trade.[7] Ports are critical infrastructures, given their strategic nature, and are vulnerable to political, socioeconomic, technological, environmental, and physical threats. In addition, inter-state disputes and geopolitical crises could also directly impact port security. For example, the Russia-Ukraine armed conflict has seriously impacted the maritime transport sector: the closure of Ukrainian ports has caused major disruptions in European and other supply chains due to the lack of maritime logistics and connectivity.[8] Geopolitical tensions are not new to Southeast Asia maritime areas; with frequent encounters between law enforcement vessels and/or navies in the disputed South China Sea waters, the major ports in the region need to be proactive in handling any potential crisis or security threats.

There are a range of security threats at seaports such as piracy, armed robbery, terrorism, drug smuggling and human trafficking, cargo theft, illegal fishing, and environmental damage. Ports have been facing significant challenges due to those security threats and the ongoing modernisation and digitalisation have only made it more difficult to address cybersecurity risks. Criminals are becoming more sophisticated in committing traditional physical security threats such as cargo theft, piracy, and drug smuggling by remotely taking control of the digital port management systems.

IT IS REPORTED THAT ABOUT 90% OF ALL GLOBAL TRADE FLOWS THROUGH JUST 39 BOTTLENECK REGIONS IN THE WORLD.

Southeast Asia is located at one of the most strategic sea lines of communication in terms of global trade, food, and energy security.[9] It is also a home to the world's busiest ports strategically located along the Straits of Malacca, such as the Port of Singapore, Port Klang, and Port of Tanjung Pelepas in Malaysia, and Belawan Port in Indonesia. Any disruptions caused by cyber attacks against these ports will have catastrophic impacts on the global maritime supply chain. Ports across Southeast Asia are leveraging advanced technologies to improve their capacity and efficiency in handling large volumes of cargo. For example, the Ministry of Transport (MOT) of Malaysia recently approved plans for a smart AI container port in Negeri Sembilan, Malaysia; the MOT of Singapore has signed a memorandum of understanding (MOU) with Japan and Australia for collaborations in relation to the decarbonisation and digitisation of ports under the Green and Digital Shipping Corridor (GDSC); the MOT of Indonesia has digitised ships and goods services using the Inaportnet platform at 45 ports across Indonesia, and digital platforms are being used to track and monitor processes.[10]

While accelerating the digitalisation of port infrastructures is a priority, it is crucial to also consider the security and safety aspects of port operations as they become more vulnerable to cybersecurity risks. In addition, ports vary widely in terms of the functions and services they provide, their ownership structures (which may be public, private, or a combination of both), their size and capacity, and their geographic locations.[11] This diversity can pose challenges in establishing uniform cybersecurity standards for ports, leading to significant vulnerabilities arising from gaps in cyber risk management frameworks or varying levels of digitalisation.

Moreover, ensuring legal certainty relating to port cybersecurity is crucial as it may cause companies to avoid operating in that jurisdiction, which would lead to reduced activities and subsequent economic damage.[12] Therefore, there is a critical need for systematic and uniform regulatory and compliance mechanisms to ensure the cyber resilience of ports in each country. This paper will provide recommendations for regulatory and policy readiness concerning cybersecurity in major port countries across Southeast Asia.

TECHNOLOGICAL ADVANCEMENTS AND CYBERSECURITY IN PORTS

Digital transformation is rapidly reshaping ports worldwide by modernising logistics, streamlining operations, and boosting supply chain efficiency. Over 20% of the world's 4,900 ports have already adopted advanced digital systems to enhance connectivity. In addition, many Southeast Asian countries are leveraging automation, blockchain, and IoT technologies to improve operational efficiency, sustainability, and cargo traceability.[13]

PORT DIGITALISATION

The digitalisation of ports is also known as Ports 4.0, a new era of intelligent ports that use advanced technology to improve their operations and offer more efficient and sustainable services. Some of the key technologies used in Ports 4.0 include artificial intelligence (AI), the Internet of Things (IOT), robotics, automation and cloud computing.[14]

The port industry is rapidly evolving through digital transformation, which introduces new risks alongside increased connectivity between ports.[15] Digital transformation in ports involves two processes: (i) digitising, which converts documents like contracts and bills of lading into digital formats, and (ii) digitalisation, which automates business processes and operations.[16] In addition, the growing reliance on Information Technologies (IT) and Operational Technologies (OT), along with their convergence in port operations, exposes ports to cybercriminal threats.[17]

Most commercial ports have embraced digital systems across multiple layers: physical (Gates Storage, OT End Devices, network (Internet, Satellites, WiFi) systems and software (Data Identification, Port Community Systems), electronic data (Trade data, Coastal data), services (Invoicing, Container Management), user functions (Personnel, Port Authorities, Maritime Companies, Ships) and processes (loading, unloading). Each of these layers is at risk of malicious cyber intrusion by various methods of infiltration depending on the vulnerabilities identified and which asset is a target of the attack. These interconnected layers underscore the extensive impact a cyber attack could have on the entire port system.[18]

PORT AUTOMATION

There is a growing interest in the automation of container terminals to improve quayside and landside productivity. Port terminals are more likely to be automated since this directly improve cost, efficiency, safety, and reliability performance indicators. The demands from port users are increasing in terms of productivity and efficiency of operations: shipping companies want containers to be loaded and unloaded as quickly as possible from ever-larger vessels to minimize the time those vessels spend in ports, and deliver cargo to shippers who need to meet just-in-time inventory management strategies.[19] It was estimated that about 71 container terminals around the world, representing 8.3 % of all main container terminals, were either fully or partially automated as of mid-2024, and this number is likely to grow in the future.[20]

As part of port automation, systems such as gantry cranes, which handle container unloading, and gates controlling truck movement within port areas are now operated through interconnected software and processors. In addition, containers are often equipped with GPS trackers to monitor their positions on ships or within terminal yards. Consequently, a cyberattack that manipulates or disables GPS signals or disrupts the functioning of cranes and gates can cause major operational disruptions and require significant time to restore normal activities.[21] The significance of cyber risks against automated terminals was demonstrated by the NotPetya cyber attack in 2017, which shut down 76 global port facilities and forced Maersk to suspend operations at multiple terminals worldwide, causing an estimated financial loss of 300 million USD.[22] Protecting automated terminals from cyber risks can be even more challenging due to their complex industrial control systems connecting mechanical equipment, sensors, and data networks, which are all vulnerable to cyber threats. Moreover, identifying and fixing software bugs can take months or years, as these systems must remain operational while managing continuous cargo movements.[23]

CYBER CRIMINALS AND THEIR MOTIVATIONS

Cyber threat actors targeting ports include state and non-state actors such as cybercriminals, terrorists, and hacktivists. Cybercriminals typically use ransomware to gain financial benefits, as seen in the July 2023 LockBit ransomware attack on Japan's largest maritime port, which disrupted cargo operations.[24] Terrorists may target ports, as critical infrastructure, to disrupt supply chains or cause physical damage, particularly with operational technologies that can be remotely controlled. Hacktivists, often linked to political or ideological causes, may target ports or their operators.

Cyber espionage is another significant threat, driven by both criminal groups and states, especially amid rising geopolitical tensions in Southeast Asia. Cyber espionage involves stealing sensitive information or sabotaging operations, leading to financial losses and operational disruption.[25] While the use of destructive cyber attacks or cyber warfare by states is not anticipated, any disruption – whether cyber or physical – could severely affect global trade and supply chains, causing significant financial damage.

RISKS AND VULNERABILITIES OF MODERN PORT OPERATIONS

The security landscape of ports has changed over the years along with their increased modernisation through the integration of new technologies such as Internet of Things (IoT), big data, cloud computing and artificial intelligence (AI).[26] Anything that is smart and connected to the internet can be hacked, and anything claiming to be 'artificially intelligent' can create havoc if the underlying algorithms are flawed. In the era of automation across every sector, it is essential that risk assessments are undertaken thoroughly and through an automation lens.[27] This means that the more port systems and operations are automated, the stronger the automated cyber defence is required to be.

The digitalisation of ports has attracted both new and traditional threat actors, leading to an increase in cyber attacks targeting maritime infrastructure worldwide. Cybercriminals have used digital tools to facilitate traditional threats like theft and smuggling, as exemplified by the multi-stage cyber-physical attack at the Port of Antwerp from 2011 to 2013, which enabled drug traffickers to access containers through compromised systems and physical break-ins.[28] More recently, in 2023, a cyberattack at the Port of Nagoya disrupted operations for several days when a system failure accompanied by a ransom demand prevented containers from being loaded or unloaded.[29] In November 2024, the DP World Australia attack led to the closure of its port operations in Melbourne, Sydney, Fremantle and Brisbane, resulting in containers and cargo being stuck on the docks.[30] In December 2024, the Port of Rijeka in Croatia was hit by a cyber attack, for which the 8Base ransomware group claimed responsibility. The attack resulted in the theft of sensitive information such as financial data, personal details, employment contracts, and non-disclosure agreements.[31]

The impacts of cyber attacks can vary greatly in severity, ranging from a minor inconvenience to a complete shutdown of port operations, leading to financial loss, reputation or competitiveness loss, fraud, trafficking, cargo theft, system outages, and even personal injury or death, due to compromised OT systems causing unexpected equipment malfunctions that could endanger the industrial environment. For example, the DP World Australia cyber attack led to the closure of port operations in four different locations,[32] while in another lesser incident, a Denial of Service (DDoS) attack on the websites of several Belgian municipalities and ports (including Antwerp and Zeebrugge) overwhelmed servers with excessive requests, rendering them inaccessible.[33]

INTERNATIONAL AND ASEAN FRAMEWORKS RELEVANT TO CYBERSECURITY OF PORTS

This section reviews relevant international and ASEAN frameworks applicable to port cybersecurity that provide an important basis for shaping national policy approaches and strengthening legal and regulatory frameworks for port cybersecurity governance.

CONVENTION ON CYBERCRIME, 2001

The main objective of the Convention on Cybercrime (Budapest Convention) 2001 is to pursue a common criminal policy to protect the society against cybercrime, through adopting appropriate legislation and fostering international cooperation.[34] It requires States to take substantive and procedural criminal law measures to fight against cybercrimes. The Convention also facilitates extradition and mutual assistance for States to enhance coordination between their relevant agencies to fight cybercrimes.[35] Parties to the Convention include the Philippines.[36] A number of activities compromising port cybersecurity, such as illegal access to a computer system, interception without rights of non-public transmissions of computer data, interference with computer data without right, and misuses of devices are forbidden by the Budapest Convention.[37]

UNITED NATIONS CONVENTION AGAINST CYBERCRIME, 2024

The United Nations Convention against Cybercrime (full title: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes) will be open for signature in 2025.[38] The Convention's purposes are to promote measures to combat cybercrime more efficiently and effectively; strengthen international cooperation in combating cybercrime; and support capacity-building to combat cybercrime.[39] It concerns the prevention, criminalisation, jurisdiction, procedures, and international cooperation relating to cybersecurity offences.[40] Many activities affecting port cybersecurity are criminalised under its framework, namely: illegal access to a communication and information system, interception by technical means of non-public transmissions of electronic data, interference with electronic data and communication and information systems, and misuse of devices.[41]

ISPS CODE

The International Convention for the Safety of Life at Sea, or SOLAS Convention, serves to determine minimum standards for the ship's safety.[42] Under SOLAS, an International Ship and Port Facility Security (ISPS) Code was adopted to prevent security incidents affecting ships and ports.[43] The Code is divided into two parts. The mandatory part outlines maritime and port security-related requirements which States, port authorities and shipping companies must adhere to. With regards to port security, a port facility is required to act upon the security levels set by the State within whose territory it is located. The port facility security assessment shall also be carried out. Furthermore, a port facility security plan (based on a security assessment) shall be developed and maintained for each facility.[44] The recommendatory part provides guidelines on how to meet the requirements and obligations set out within the provisions of the former part. For instance, it provides that States can establish designated authorities within government to undertake port security duties.[45] The ISPS Code provides for the general regime of security of ports, which could also apply to cybersecurity.

IMO RESOLUTIONS ON MARITIME CYBERSECURITY

IMO has developed a set of interim guidelines on maritime cyber risk management, with the latest one adopted in 2022.[46] The IMO guidelines provide recommendations on maritime cyber risk management to safeguard shipping from cyber threats and vulnerabilities. According to the IMO, vulnerable systems could include cargo handling and management systems, power control systems, and access control systems which are present in ports.[47] Under the guidelines, effective cyber risk management starts at senior management level, whereby a culture of cyber risk awareness should be embedded into all levels of an organisation. Additionally, IMO adopted Resolution MSC 428 (98) 2017 encouraging administrations to ensure that cyber risks are appropriately addressed in existing safety management systems.[48]

Guides and standards relating to maritime cybersecurity recognised by IMO

IMO recognised three guides and standards that could be used to port cybersecurity.

ISO/IEC 27001:2022

ISO/IEC 27001:2022 on Information Security Management System is a standard jointly published by the International Organisation for Standardisation and the International Electrotechnical Commission. The Standard provides companies with guidance for establishing, implementing, maintaining, and improving an information security system.[49] Although this Standard is not particularly designed for the maritime industry, its guidelines apply to improve port cybersecurity.

IAPH Cybersecurity Guidelines for Ports and Port Facilities

In 2021, IAPH released foundational guidelines for cybersecurity of ports and port facilities, developed jointly by the International Association of Ports and Harbors (IAPH) and the World Bank to support global ports to comply with IMO's Guidelines on Maritime Cyber Risk Management.[50] The guidelines are intended for use by the Chief Executive Officer and C-suite executives.[51] They are designed to foster greater collaboration within their organisation, as well as more broadly with their local, regional, national, and international partners.

In 2025, IAPH released the *Cyber Resilience Guidelines for Emerging Technologies in the Maritime Supply Chain,* which not only outline measures for detecting, mitigating, and protecting against cyber threats, but also emphasise the importance of training, capacity building, and the development of supportive legislation to ensure a resilient maritime supply chain.[52] The key elements of the updated IAPH Guidelines, released in 2025, emphasize integrating cybersecurity by design in the early stages of planning and deployment of emerging technologies, ensuring that risks are assessed holistically, including for technologies that are yet to be adopted. They also highlight the need for technology-specific protections, continuous training, and legal and policy updates to enable a cyber-secure and resilient maritime supply chain.[53]

The United States NIST Cybersecurity Framework

The NIST Cybersecurity Framework was developed by the United States National Institute of Standards and Technology (NIST) to enact the President's Executive Order 13636/2013, which calls for the development of a voluntary Cybersecurity Framework to manage the cybersecurity risk of critical infrastructure services.[54] This framework can be used by organisations based on their risks, threats, vulnerabilities, and risk tolerances.[55]

ASEAN Guidelines and Plans relating to Cybersecurity

ASEAN has developed a number of guidelines and a plan to help ASEAN member states (AMS) to improve their cybersecurity.

The Critical Information Infrastructure Protection Guidelines, 2016

The Critical Information Infrastructure Protection (CIIP) was adopted under the ASEAN framework in 2016.[56] These guidelines are intended to be used as a reference for AMS regulators to develop national CIIP policies for their critical sectors. It contains provisions for the development of CIIP policies, the establishment of an information security policy, and guidelines for security standards.[57]

ASEAN Data Management Framework, 2021

The *ASEAN Data Management Framework: Data Governance and Protection throughout the Data Lifecycle* (DMF) was endorsed by ASEAN in 2021[58] to provide non-binding guidance in data management for businesses within AMS. For cybersecurity, the DMF suggests the use of the NIST Framework as standard to guide organisations in assessing how their own data should be categorised and organised.[59]

ASEAN Digital Master Plan 2025

The ASEAN Digital Master Plan (ADM) 2025 was adopted by ASEAN in 2021 to make Southeast Asia a leading digital community with secure digital services.[60] A desired outcome under the ADM is the delivery of trusted digital services. Enabling actions agreed to achieve this outcome are building trust through enhanced security for finance, healthcare, education and government, and improved coordination and cooperation for regional computer incident response teams.[61]

ASEAN Measures to Improve Cybersecurity in Southeast Asia

As part of ASEAN efforts in promoting cooperation in cybersecurity, the ASEAN Computer Emergency Response Teams (CERT) have been established. By 2012, all AMS had their national CERTs.[62] Annual CERT Incident Drills (ACID) have been organised to test incident response procedures and strengthen cybersecurity preparedness and cooperation among CERTs in AMS and dialogue partners.[63] In 2018, the ASEAN-Japan Cybersecurity Capacity Building Centre was opened in Bangkok to train personnel from AMS to combat cyber threats.[64] In 2023, the ASEAN Defence Ministers' Meeting on Cybersecurity and Information Centre of Excellence was opened in Singapore to undertake confidence-building measures, enhancing information-sharing and capacity building among ASEAN defence establishments.[65]

This section pointed out a number of international and regional frameworks which could help Southeast Asian countries in particular to improve the cybersecurity of their ports. Four of them are mandatory: the Budapest Convention, the UN Convention against Cybercrime, the ISPS Code, and the IMO resolutions. Others are IMO- or ASEAN-recognised guidelines which were developed based on best practices worldwide on the cybersecurity of information systems, critical infrastructures, ports and data management. If all these international and regional frameworks were to be followed by Southeast Asian countries, the cybersecurity of ports in the region would significantly improve.

The next section of the report looks at major shipping countries in Southeast Asia, namely Singapore, Malaysia and Indonesia, to identify the gaps in their legal and regulatory framework governing port cybersecurity.

REGULATING PORT CYBERSECURITY: PRACTICES OF SINGAPORE, MALAYSIA AND INDONESIA

As major port countries in Southeast Asia accelerate the digitalisation of port infrastructures, it is crucial to also address the security and safety aspects of port operations. It is essential to implement a systematic cyber risk management framework and ensure regulatory readiness, in compliance with existing international frameworks and guidelines discussed in Section III. This section evaluates port digitalisation, cybersecurity measures, and regulatory practices in three major Southeast Asian port countries: Singapore, Malaysia, and Indonesia. The aim of this evaluation is to understand the regulatory landscape of port cybersecurity, identify gaps in their current efforts to ensure and implement robust cybersecurity requirements across their port sectors.

SINGAPORE

Port Management Structure

The port of Singapore, the busiest port in Southeast Asia and second globally after Shanghai,[66] is managed by the Maritime Port Authority of Singapore (MPA), a statutory body under the Ministry of Transport.[67] MPA governs and regulates Singapore's port and maritime ecosystem, while PSA International[68] operates and manages the terminals within the MPA's regulatory framework. MPA and PSA form a complementary structure: while MPA ensures safety, compliance, and strategy, PSA drives operational excellence and innovation.

As the regulator of the biggest port in Southeast Asia, MPA and its various initiatives are considered the best practice model in the region as it enhances safety, security, environmental protection, and policy development by close collaboration with industry, research communities, and other relevant agencies. In 2025, Singapore's port handled a record 44.66 million twenty-foot equivalent units (TEUs), surpassing the 41.12 million TEUs processed in the previous year.[69]

Digitalisation and automation

In order to stay competitive in maritime transport and international trade, Singapore has implemented key initiatives forming the digital port ecosystem, including: Singapore Maritime Digital Hub (SG-MDH); digitalPort@G™(Portal for One-stop Regulatory Transactions); and digitalOCEANS™ (Open/Common Exchange and Network Standardisation).[70] All these initiatives form the core of Singapore's digital port ecosystem, which helps to reduce the administrative burden for shipmasters during port calls so that they can focus on the primary responsibility of navigating ships safely. Singapore also implements digitalPORT@SGTM in line with the Maritime Single Window (MSW) as mandated by the IMO[71], which streamlines vessel, immigration, and port health clearances across multiple agencies into a single application consolidating 16 separate forms. Here, shipmasters and ship agents from more than 550 shipping companies can submit, track, and receive approval for arriving and departing ships through the portal. As a result, the industry can save up to 100,000 man-hours per year.[72]

In addition, the MPA is also planning to use artificial intelligence (AI) and digital twins to optimise vessel route planning to enhance safety and reduce emissions in maritime operations. The digitalPORT@SG™ Just-in-Time (JIT) Planning and Coordination Platform will facilitate the optimal arrival and departure of vessels to and from the Port of Singapore, to reduce ship turnaround time as well as dwell time at anchorages before berthing.[73]

In addition, PSA Singapore is advancing its vision of building the world's largest fully automated port through the Tuas Port project, a key milestone that reinforces Singapore's position as a global maritime hub. The first phase opened in 2022 with full completion expected by 2040, doubling the nation's handling capacity and enhancing integration between sea and air transport. Currently operating eight berths, Tuas Port relies on Automated Guided Vehicles (AGVs) and advanced technologies such as AI, data analytics, and robotics to boost efficiency, support supply chain resilience, and create new employment opportunities.[74]

Existing Initiatives on Port Cybersecurity

The Relevance of the Cybersecurity Act 2018

The Cybersecurity Act 2018 is a legislation that provides various cybersecurity-related provisions, including requiring and authorising measures to prevent, manage, and respond to cybersecurity threats and incidents. It aims to provide a framework for the designation of Critical Information Infrastructure (CII), providing owners with clarity on their obligations to proactively protect the CII from cyber attacks.[75] The CII sectors in Singapore include energy, water, banking and finance, healthcare, transport (which includes land, maritime, and aviation), infocomm, media, security and emergency services, and government.[76]

The provisions under this Act are particularly relevant for cyber attacks against or through computer systems that jeopardise or adversely affect their cybersecurity or the cybersecurity of another computer or system.[77] Although this legislation is a general cybersecurity law in Singapore, it is also relevant to certain maritime-related operations and infrastructures, including ports and shipping. For instance, "services related to maritime" are classified as essential services, for which cybersecurity responses are mandated by the Commissioner. These services include monitoring and management of shipping traffic; container terminal operations; general and bulk cargo terminal operations; cruise and ferry passenger terminal operations; pilotage, towage, and water supply; bunker supply; salvage operations; and passenger ferry operations.[78]

Although the Cyber Security Act can be relevant for cybersecurity incidents against IT or computer systems of ports and terminal operations, there remain gaps in extending this protection to the broader spectrum of IT and OT used across other port operations and relevant infrastructure.

MOUs and multi-stakeholder collaborations

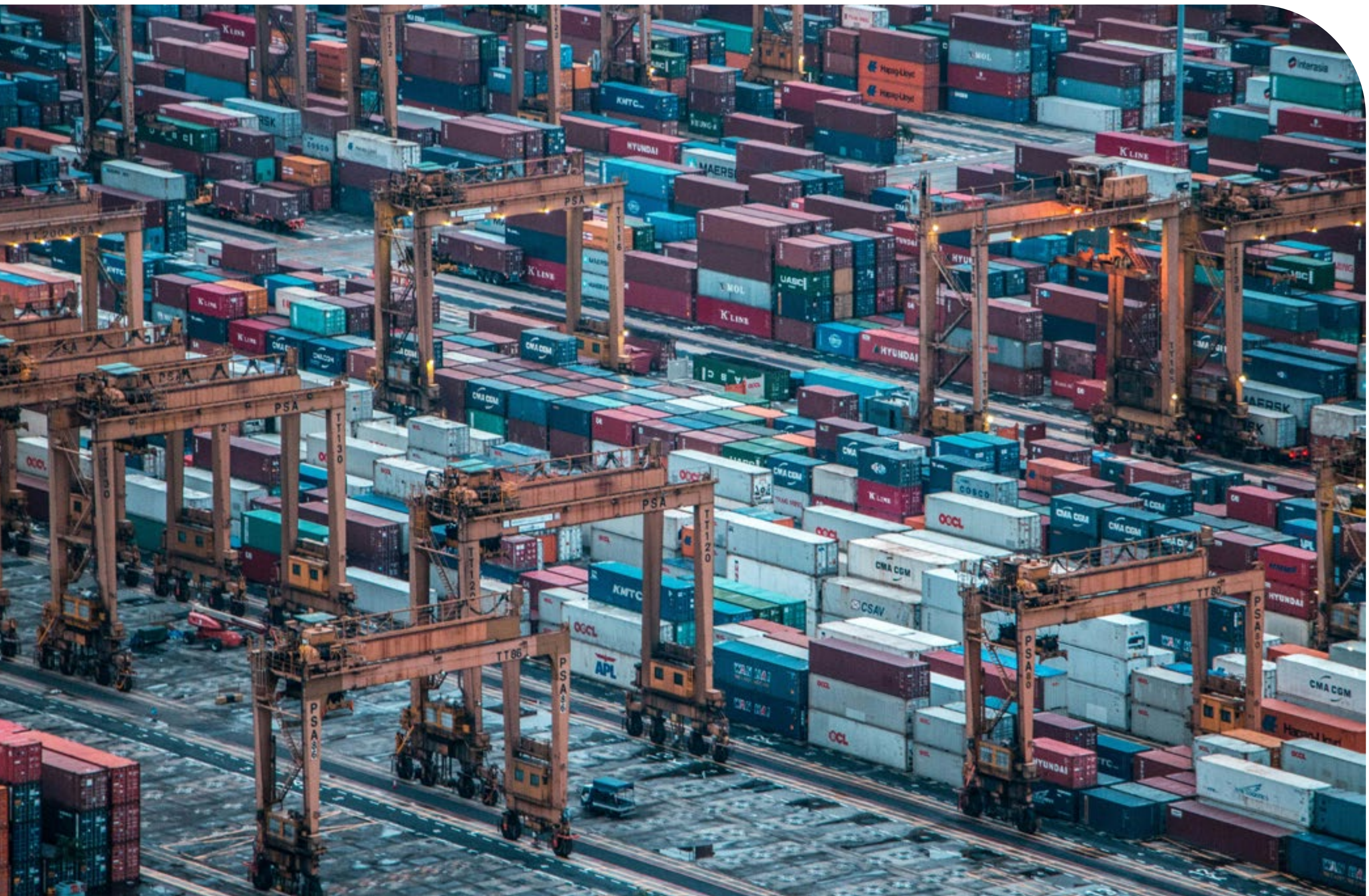
- *Joint Cyber Training Exercises* (MoU between MPA, Taltech, Foundation CR14, SMI and SUTD): The MoU was signed between MPA, Tallin's University of Technology (TalTech, Estonia), Foundation CR14, the Singapore Maritime Institute (SMI), and the Singapore University of Technology and Design (SUTD). The MoU aims to enhance cybersecurity in the maritime industry, in particular joint cybersecurity research and development, test-bedding, and skills training projects.[79]
- *Information Sharing and Creating Cybersecurity Talent Pipeline* (MoU between MPA, SSA, SIT and SUTD): Another MOU was signed between MPA, Singapore Shipping Association (SSA), Singapore Institute of Technology (SIT), and SUTD to improve collaboration and information sharing on cybersecurity among maritime companies, develop maritime cybersecurity capabilities, and strengthen the cybersecurity talent pipeline. This is an initiative under the Maritime Cybersecurity Roundtable[80] spearheaded by SSA in collaboration with MPA and industry.
- *Innovation, Digitalisation, and Cybersecurity* (MOU between MPA and Microsoft): More recently, as part of a digitalisation effort, the MPA also signed a MoU with Microsoft on 29 July 2024 to collaborate in innovative technologies including cloud computing, artificial intelligence (AI), data analytics, robotics, and cybersecurity, as well as support the adoption and development of digital and green solutions for the maritime industry.[81]

Expansion of Maritime Cybersecurity Operation Centre (MSOC)

In 2019, the MPA launched the 24/7 Maritime Cybersecurity Operations Centre (MSOC), to be operated by ST Engineering. MSOC will provide early detection, monitoring, analysis, and response to potential cyber attacks on maritime critical information infrastructure. It will also identify and track cyber attacks by analysing activities within the IT environment, detecting anomalies and threats, and responding with suitable technological solutions.[82] As an expansion of MSOC, MPA has launched the Maritime Cyber Assurance and Operations Centre (MCAOC) to provide real-time cyber monitoring and threat information, enabling companies to respond early to cyber risks. By pooling cyber monitoring and information-scanning capabilities, MCAOC is expected to help participating companies save about S$200,000 annually, and 16 companies have joined the initiative to date.[83]

MPA-led annual cybersecurity tabletop exercise (TTX)

In 2024, ten companies from across various maritime sectors participated in the MPA-led annual cybersecurity tabletop exercise (TTX), together with international participants from the Port Authorities CIO Cybersecurity Network (Pacc-Net) and other like-minded ports and port authorities.[84] The TTX simulated cyberattacks affecting multiple ports across regions, and tested and validated the pilot implementation of the MPA-hosted Maritime Cyber Assurance and Operations Centre (MCAOC) capabilities, a joint MPA-industry cybersecurity operations centre.[85]



TERMINAL BURCHARDKAI
TERMINAL BURCHARDKAI
CMA CGM GEORG FORSTER
LONDON
CMA CGM

MALAYSIA

Port Management Structure

In Malaysia, the port management structure is decentralised and fragmented, unlike Singapore's integrated system under a single maritime authority. Ports in Malaysia are either federal or state-managed, each governed by their respective authorities.[86] Currently, Malaysia has eight federal ports, two of which are among the biggest in Southeast Asia: Port Klang and Port of Tanjung Pelepas (PTP). Both are now gearing towards digitalisation and automation.[87]

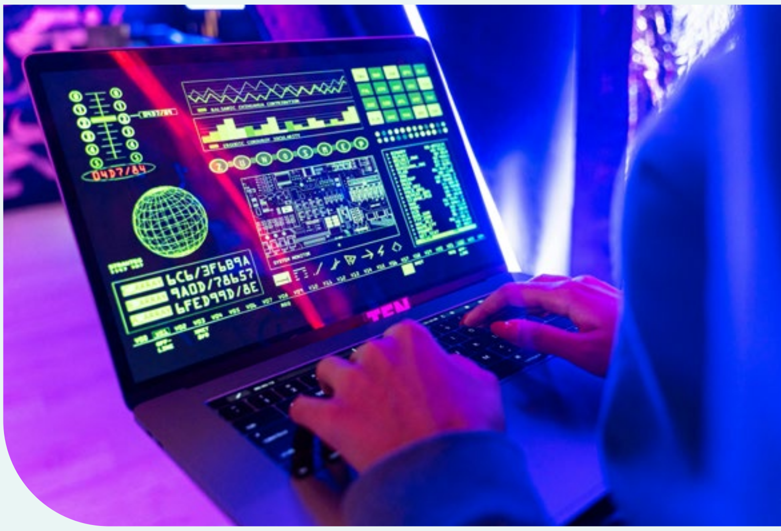
Based on port privatisation practices, port authorities are the landowners who lease the port to private operators to manage. The port authority has regulatory functions in respect of port activities such as the operation of port facilities and services offered there by licensed operators, including their quality, performance standards, and the enforcement thereof.[88] The role of port authorities in Malaysia is crucial as the regulator for the safety and security of privately managed port operations, including the digitalisation and the management of cybersecurity risks at the digitalised ports.

Digitalisation and Automation

Malaysia has kept up with the most advanced ports by automating and digitalising port operating activities in the country. Due to the significant increase in the volume of cargo handled by its ports in recent years, Malaysia is preparing to accommodate this increasing volume and for future growth. For example, West Port is undergoing a major expansion plan that will double its capacity from the current 14 million twenty-foot equivalent units (TEUs) to nearly 28 million TEUs, ensuring that Port Klang remains competitive on the global stage.[89]

One of the significant digital advancements in Malaysian ports is the Remote Physical Check System (RPS), to verify every container being loaded or unloaded from the vessels.[90] RPS is an in-house initiative developed by Port Klang and it reduces the need for physical inspections while enhancing accuracy, accountability, and speed of operations. In addition, Port Klang is also exploring other digital tools such as blockchain technology for improved tracking and tracing of shipments, automated port management systems for optimising resource allocation, and artificial intelligence to predict and manage cargo flow.[91]

The Port of Tanjung Pelepas (PTP), another major port in Malaysia and the 3rd biggest port in Southeast Asia, has also embarked on the digital makeover and is adopting advanced technologies such as AI and machine learning in its operations. An example is MarineM, an AI-powered system which can instantly reallocate resources in case a vessel's ETA changes, thus reducing waiting times and making PTP more resilient in the face of congestion.[92] In addition, PTP now has real-time data on vessel movements, container status, and overall terminal operations.[93] For example, PTP has recently implemented a new Terminal Truck Optimisation (TT-O) solution to take a smarter approach to truck movements across multiple zones; PTP drivers now receive their job assignments 44 percent faster, leading to a 13 percent reduction in truck cycle time. In addition, TT-O also enables dual cycle handling and prioritisation based on each crane's performance, maximising quay crane moves and lowering wait times.[94]



While embracing the need for advanced technologies and digitalisation, PTP also recognizes that cybersecurity and data security is a significant challenge with the concern over handling vast amount of sensitive data, cyberattacks, and potential privacy violations in the port's digitalisation process.[95]

Existing Initiatives on Port Cybersecurity

Relevance of the Cyber Security Act 2024

The recently adopted Cyber Security Act 2024 does not directly address the cybersecurity aspect of Malaysian ports as it only considers transportation as one of the sectors of national critical information infrastructure. Under this Act, a "cybersecurity threat" is defined as any act or activity conducted on or through a computer or computer system, without lawful authority, that may imminently jeopardize or adversely affect the cybersecurity of that system or another connected one.[96] Consequently, the legislation primarily addresses incidents targeting IT or computer systems, leaving a gap in coverage for the broader integration of IT and operational technology (OT) infrastructures within port operations.

Lack of Sector-Specific Initiatives on Port Cybersecurity

Although major ports such as Port Klang and Port of Tanjung Pelepas have been digitalised to a certain extent and continuing to invest in port infrastructure for further automation and digitalisation of port operations, unlike Singapore, Malaysia has yet to come out with sector-specific legal, regulatory, and risk management efforts at the national level. Currently, ports such as PTP have their internal cybersecurity department which handles and monitors cybersecurity risks; the port conducts social engineering exercises on email phishing, as well as phone phishing trials with staff members.[97]

INDONESIA

Port Management Structure

Indonesia has eight major ports supporting international trade[98], with the Port of Tanjung Priok serving as the country's largest and busiest hub[99]. Port operations nationwide are managed by PELINDO, the sole state-owned enterprise, under long-term concessions from the Ministry of Transport. PELINDO subcontracts operations to terminal operators such as JICT and NPCTI, while retaining responsibility for infrastructure maintenance. To enhance efficiency, PELINDO is increasingly adopting technologies like AI and IoT to automate and integrate port operations.[100]

As for the regulation relating to ports, the Harbor Master and Port Authority Office (Kantor Kesyahbandaran dan Otoritas Pelabuhan [KSOP]) is responsible as a technical implementing unit within the Ministry of Transportation. Each port has a port authority, which coordinates government activities at the port, including customs, immigration, and quarantine. The port authority also regulates, controls, and supervises port activities. There are four main port authorities in Indonesia: Ports of Belawan, Tanjung Priok, Tanjung Perak, and Makassar.[101]

Digitalisation and automation

The Indonesian port sector is rapidly adopting the smart port concept to enhance performance and operational efficiency. There have been several initiatives for the digitalisation of port operations in Indonesia through advanced systems like INAPORTNET (internet-based electronic service information system), SIMLALA (online naval traffic permit service application), SIJUKA (information system for approval of use of foreign vessels)[102], and the National Logistics Ecosystem (NLE), among others. These innovations aim to streamline logistics processes, boost efficiency, and strengthen Indonesia's maritime infrastructure. One of the significant purposes of port digitalisation in Indonesia is to eradicate corruption by enhancing transparency, boosting operational efficiency, and aligning with broader efforts to strengthen governance in the port sector.[103]

Smart ports in Indonesia increasingly leverage advanced technologies such as Internet of Things (IoT) devices, including sensors and wireless technologies, to optimise service efficiency and enhance operational capacity. In 2022 the coordinating minister for Maritime Affairs and Investment announced that Indonesia's target was to transform 149 ports into smart ports; these comprise 112 ports under state-run port operator PT Pelindo Indonesia (Persero) and 37 ports under several agencies, including private parties and the Ministry of Transportation. There were 14 ports certified as green and smart ports in 2022.[104]

State-owned port operator PELINDO is spearheading efforts in port digitalisation. In 2023, PELINDO introduced automatic gates at 13 ports, building on its earlier success with cashless system implementations at Banten, Tanjung Pandan, Sunda Kelapa, Banjarmasin, and Gresik. Several key Indonesian ports, including Kuala Tanjung, Cikarang Dryport, Tanjung Priok, Semarang Container Terminal, and Teluk Lamong have initiated smart technology upgrades.[105] In addition, Batu Ampar Port is being developed as a smart port and International Trans-shipment Port (ITP), collaborating with technology providers to integrate logistics services into a unified application. This aligns Batu Ampar with global Port 4.0 trends and enhances cargo handling efficiency.[106]

Although many Indonesian ports have adopted digitalisation, inconsistencies in implementation highlight the need for standardised approaches to maximise efficiency. As of 2023, INAPORTNET had been fully deployed in only 109 out of 1,145 ports, indicating delays in achieving nationwide integration. In addition, studies also suggest that digitalisation has yet to yield a significant impact on business sustainability, possibly due to the limited digital maturity of Indonesian ports.[107]

Technologies like automation systems, cargo tracking, real-time asset monitoring, remote-controlled cranes, Automated Guided Vehicles (AGVs), drone inspections, and strong cybersecurity measures are crucial for improving port operations. Furthermore, there is a pressing need to enhance the IT skills of port staff, as training opportunities are currently insufficient. Expanding training programs focused on port technologies is vital for developing a skilled workforce that can successfully implement digital innovations.[108]

Existing initiatives on port cybersecurity

Relevant national regulation on cybersecurity at ports

Unlike Singapore and Malaysia, Indonesia does not yet have a standalone cybersecurity law. However, it is currently drafting the Cybersecurity and Resilience Bill (RUU KKS) to establish a comprehensive national legal framework for cybersecurity. Cybersecurity matters in Indonesia are currently governed by the Electronic Information and Transactions (EIT) Law and the Personal Data Protection (PDP) Law.[109] Other relevant regulations include Presidential Regulation No. 47 of 2023 on National Cyber Security Strategy and Cyber Crisis Management (PR 47/2023), which is further detailed by BSSN Regulation No. 1 of 2024 on Cyber Incident Management (BSSN 1/2024) and BSSN Regulation No. 2 of 2024 on Cyber Crisis Management (BSSN 2/2024).[110] These BSSN regulations apply specifically to Vital Information Infrastructure (VII) providers, which include government agencies, business entities, and organisations that own or operate such infrastructure. Under Presidential Regulation No. 82 of 2022, transportation is designated as one of the VII sectors. Consequently, maritime transportation, including ports, is only indirectly governed under this regulatory framework.[111]

Other relevant initiatives

One of the significant aspects of Indonesia's efforts to strengthen port cybersecurity is its focus on applying the ISPS Code to address potential cyberattacks on port facilities. This approach aims to ensure that ports are prepared to respond effectively to incidents such as system shutdowns or acts of sabotage, supported by well-established communication channels among stakeholders at Tanjung Priok Port. The Ministry of Transport has also placed increasing emphasis on enhancing cybersecurity standards and practices in Indonesian ports, particularly concerning the technical and regulatory dimensions of implementing the ISPS Code.[112]

The very first training and implementation of the ISPS Code against cyber attacks was initiated by the Directorate General of Sea Transportation of the Ministry of Transportation, together with other port related agencies in Tanjung Priok. The training was entitled "Joint Exercise ISPS Code Port Facilities Cyber Attack and Traffic Impact" and it was held at the Port of Tanjung Priok Port Maritime Museum on 29 February 2024 with the aim to overcome disruptions and maintain the smooth flow of goods in case systems such as Inaportnet go down. This joint exercise was a highly collaborative and multidisciplinary event with participation from various key stakeholders from law enforcement, security and industry, such as port authorities and operators, cybersecurity and IT experts, Indonesian Navy, Police, Port Facility Security Officers (PFSO), Company Security Officers (CSO) as well as the Embassies of the United States and Australia for international cooperation.[113]

Existing legal and regulatory landscape in Singapore, Malaysia and Indonesia: Gaps and Challenges

Singapore has firmly positioned itself as a regional leader in maritime cybersecurity, supported by strong sector-specific initiatives and active collaboration among government agencies, industry players, and research institutions. Its streamlined port management structure, primarily under MPA and PSA International, enables cohesive governance and effective implementation of cybersecurity measures. Singapore's approach is marked by cross-sector cooperation and alignment with international standards, serving as a model for other nations seeking to strengthen resilience in their maritime domains.

In contrast, Malaysia's fragmented port management system, involving multiple authorities and terminal operators, results in uneven levels of digitalisation and cyber risk management across ports. To address this, establishing uniform national standards and guidelines on cyber risk management and response protocols is essential. Enhanced coordination and real-time information sharing between digitalised ports would also enable Malaysia to respond more effectively to emerging cyber threats and ensure consistency across the sector.

Indonesia's structure differs again, as the Ministry of Transportation holds central regulatory authority, while PELINDO – the state-owned port operator – oversees most operational functions. Despite this centralisation, closer engagement with private stakeholders and terminal operators remains vital to ensure standardised implementation of cybersecurity frameworks and best practices across Indonesian ports.

Overall, port privatisation complicates regulation, as diverse actors with varying cybersecurity capacities become involved. While all three countries recognise Critical National Information Infrastructure (CNII), port infrastructure is not explicitly defined within it. Given the complex and interconnected nature of ports, linked to ships, logistics networks, and external systems, there is a pressing need for a dedicated legal framework addressing cybersecurity in ports and the broader maritime infrastructure.

The next section of the report suggests a number of concrete policy recommendations for improving port cybersecurity governance in Southeast Asia.

POLICY RECOMMENDATIONS

UPDATING NATIONAL CYBERSECURITY LAW TO COVER CYBERSECURITY OF PORTS

Among the countries studied, only Singapore mentions port cybersecurity in national law. Having legal provisions on the cybersecurity of ports could help strengthen their readiness against cyber risks. Such provisions increase the sense of duty of port operators to safeguard the cybersecurity of ports. Furthermore, they serve as the basis for the adoption of measures targeting port protection specifically.

HARMONISING NATIONAL LAW RELATING TO THE CYBERSECURITY OF PORTS

In addition to updating national laws to include the cybersecurity of ports in relevant legal frameworks, Southeast Asian countries should also harmonise relevant provisions to ensure a seamless protection throughout the region. The harmonisation should concern particularly equipment standards, safeguard procedures, and responses to incidents. This would ensure that all regional countries have the same level of protection in terms of port cybersecurity. Singaporean law on protecting the cybersecurity of essential maritime service could serve as a model for other countries in the region.

COMMISSIONING MANDATORY CYBERSECURITY AUDIT FOR PORTS

From the analysis of the three case studies of Indonesia, Malaysia and Singapore, it seems that no mandatory cybersecurity audit has yet be commissioned for national ports. Southeast Asian countries could require port operators to commission cybersecurity audits for their ports. These audits would help operators check and address vulnerabilities in the facilities' information system. The ISPS code could also help if it included cybersecurity in the security plan of port facilities. As countries have to conduct regular security assessments for ports, they can take the opportunity to check and deal with potential cyber threats affecting them.

ORGANISING CYBERSECURITY DRILLS FOR PORTS

This is another lesson Southeast Asian port authorities could learn from their Singaporean counterpart. Cybersecurity drills help test and improve the response readiness of ports against cyber threats. In addition to drills organised at the national level, cross-border simulation scenarios could be developed under the annual ASEAN CERT Incident Drills to evaluate interconnectivity vulnerabilities between AMS.

ESTABLISHING UNITS SPECIALISED IN CYBERSECURITY RESPONSE IN PORTS

Specialised units dedicated to responding to cybersecurity incidents in ports could be established. They could help ensure a quick and effective reaction to all cybersecurity threats so that ports can operate without interruption. The unit could be organised across two levels. First, a group could be established at the national level to help all ports in the country improve their cybersecurity. In addition, there should be personnel dedicated to cybersecurity in each major port for a localised response.

ESTABLISHING PUBLIC-PRIVATE PARTNERSHIPS FOR CYBERSECURITY OF PORTS

Establishing public-private partnership to improve the cybersecurity of ports is also a good practice from Singapore. This helps administrations to pull together expertise and resources from all stakeholders to secure national ports. Such partnerships could also be developed between the ASEAN Cybersecurity and Information Centre of Excellence and the Federation of ASEAN Shipowners' Association to help formulate an ASEAN approach on the matter.

DEVELOPING A SET OF SOUTHEAST ASIAN GUIDELINES FOR PORT CYBERSECURITY

There has been only one set of international guidelines for cybersecurity of ports so far: the IAPH Cybersecurity Guidelines for Ports and Port Facilities. These guidelines are neither sufficient to cover all aspects of port cybersecurity nor well-suited to the Southeast Asian context. First, these are designed primarily for ports executives' use, and cover mostly inter-institutional collaboration aspects. Second, they do not take into consideration the level of development of port industry as well as the involvement of different stakeholders in the process of port governance in Southeast Asia. For these reasons, ASEAN could take the initiative to develop a set of Southeast Asian Guidelines for Port Cybersecurity to provide more appropriate guidance to port administrations and industries in the region.

PROMOTING CYBERSECURITY INSURANCE FOR PORTS

Cyber insurance has been used to mitigate the risk of cyber-criminal activities.[114] This is particularly useful for ports to cover losses from cyberattacks, as the damage resulting from these could reach billions of US dollars. However, having cyber insurance does seem to be a common practice by port managers in the region yet. For this reason, administrations in Southeast Asia could push port operators to acquire it. The insurance policy could also be tied to the safeguard of the cybersecurity of ports, so that if operators adhere well to standards of cybersecurity the insurance premium may be reduced.

LEARN FROM RELEVANT BEST PRACTICES

International best practices provide useful guidance for strengthening port cybersecurity in Southeast Asia. The EU's Agency for Cybersecurity, in its Port Cybersecurity Report (2019), recommends risk-based governance, continuous vulnerability assessment of IT and OT systems, and coordinated information sharing among port stakeholders.[115] The U.S. Coast Guard issued a final rule on in January 2025, effective 16 July 2025, establishing baseline cybersecurity requirements to safeguard the Marine Transportation System (MTS). This final rule builds on previous updates to the Captain of the Port authority, which designate cybersecurity vulnerabilities as potential threats to the security and safety of U.S. ports. The final rule requires developing and maintaining a Cybersecurity Plan, designating a Cybersecurity Officer (CySO), and taking various measures to maintain cybersecurity within the MTS.[116] The United Kingdom's Department for Transport Good Practice Guide for Ports and Port Systems (2016) stresses leadership commitment, workforce training, and layered defence mechanisms to foster a culture of cyber awareness across port operations.[117] Southeast Asian countries could draw on these examples to develop coherent national frameworks, combining regulatory oversight, public-private collaboration, and information-sharing mechanisms to enhance cyber resilience across regional ports.

JOINING INTERNATIONAL CONVENTIONS ON CYBERCRIMES

There are currently two international conventions on cybercrime, namely the Budapest Convention on Cybercrime and the UN Convention on Cybercrime. Southeast Asian countries should sign these two conventions and criminalize intentional activities affecting cybersecurity, if they have not yet done so. The UN Convention on Cybercrime was opened for signature in Hanoi, Vietnam in October 2025. As for the Budapest Convention, the Philippines has been the only signing country from Southeast Asia. The signature of the two conventions will show that they take cybersecurity very seriously and anyone trying to interfere with the safe management of data will be punished. These also provide a legal framework for closer coordination and partnership, not only among Southeast Asian countries but also between them and other regions, in investigating, incriminating and trying cybercrimes, including those targeting ports.

CAPACITY BUILDING FOR PORT CYBERSECURITY

Capacity-building programs to improve cybersecurity in Southeast Asia have been more concerned so far with cybersecurity in general, but less so with ports.[118] Thus, developing capacity-building programmes on port cybersecurity could strengthen the preparedness of port operators in dealing with cyber threats and also increase the awareness of port administration bodies about the importance of port cybersecurity. Consequently, capacity building in port cybersecurity should be designed for both port operators and administrators.

CONCLUSION

The physical security of ports has received significant attention, while the safeguarding of their digital infrastructure has remained comparatively underdeveloped. The standardisation of port cybersecurity is less advanced than that of physical security measures; this raises concerns, given that a cyber incident affecting one port can generate cascading effects across interconnected ports, supply chains, and commercial partners, potentially exceeding the impact of traditional security breaches. Existing international frameworks and soft law instruments such as the ISPS Code, relevant IMO resolutions and guidelines on maritime cyber risk management, and the IAPH Cybersecurity Guidelines for Ports and Port Facilities need to be more effectively integrated into the national regulatory frameworks governing ports across Southeast Asian countries.

It is crucial to recognise the importance of cybersecurity in safeguarding port infrastructure, given its central role in global trade and national economies. Ensuring cyber resilience in ports requires clearly identifying the agencies and institutions responsible for implementing cybersecurity measures, such as terminal operators, port authorities, relevant regulatory bodies, and any other private actors involved in offering services at ports. To strengthen governance, each country should establish a clear policy mandate requiring all national ports to adhere to cybersecurity standards and best practices. As ports form part of a nation's critical infrastructure, disruptions caused by cyberattacks can have severe consequences for both domestic economic stability and the global supply chain. Therefore, national legal frameworks should explicitly criminalise cyber intrusions and attacks targeting port infrastructure, ensuring accountability and deterrence.

IT IS CRUCIAL TO RECOGNISE THE IMPORTANCE OF CYBERSECURITY IN SAFEGUARDING PORT INFRASTRUCTURE, GIVEN ITS CENTRAL ROLE IN GLOBAL TRADE AND NATIONAL ECONOMIES.

ENDNOTES

1 Pavel Dvornák, *Transportation & Logistics 2023: Securing the supply chain,* September 2012, https://www.pwc.com/sk/en/odborne-clanky/assets/2012/2012-09_bulletin_transportation_and_logisctics_in_2030.pdf (accessed October 12, 2025).

2 LMA Consulting Group, *NBC2 WGRZ: Ever Given's ship stuck in the Suez Canal coast the economy $ 400M an hour,* March 29, 2021, https://www.lma-consultinggroup.com/nbc-2-wgrz-ever-given-ship-stuck-in-the-suez-canal-cost-the-economy-400m-an-hour/ (accessed March 15, 2025).

3 'India's Jawaharlal Nehru Port Container Terminal hit by cyberattack', February 23, 2022, https://www.ship-technology.com/news/jawaharlal-nehru-port-container-terminal/ (accessed June 18, 2025).

4 Sean Lyngaas, 'Japan's largest port hit with ransomware attack', *CNN,* July 6, 2023, https://edition.cnn.com/2023/07/06/tech/japan-port-ransomware-attack (accessed June 18, 2025).

5 Syed Rakin Rahman, 'Port of Seattle shares details of a cyberattack', *Port Technology,* September 19, 2024, https://www.porttechnology.org/news/port-of-seattle-shares-details-of-a-cyberattack/ (accessed June 18, 2025).

6 Ann Sarah Mathews, 'Port Security Measures and Their Importance', *Rcademy Word of Life,* https://rcademy.com/port-security-measures/#:~:text=global%20economy%20thrive.-,Importance%20of%20Port%20Security,port%20security%20is%20still%20crucial (accessed March 18, 2025).

7 Nippin Anand & Andrew Grainger, 'The port as a critical piece of national infrastructure' *Safety and Reliability,* 37(2–3) (2017), 106–127. https://doi.org/10.1080/09617353.2017.1334292

8 Karin Jacobs, *Russia's war on Ukraine: Maritime logistics and connectivity,* EPRS European Parliamentary Research Service, July 2022, https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733603/EPRS_ATA(2022)733603_EN.pdf

9 ASEAN, *ASEAN Maritime Outlook, First Edition,* August 2023, https://asean.org/wp-content/uploads/2023/08/AMO-1.pdf

10 South East Asia Infrastructure, *Improving Operations: Digital initiatives undertaken by SEA ports,* May 15, 2024, https://southeastasiainfra.com/improving-operations-digital-initiatives-undertaken-by-sea-ports/.

11 Oleksiy Melnyk, Oleksandr Drozdov, Serhii Kuznichenko, 'Cybersecurity in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures', *LEX PORTUS* 11(1) (2025), eISSN 2617-541X, DOI 10.62821/lp11101.

12 Ibid.

13 UOB Group, *ASEAN ports are becoming smarter and greener. Here's how it benefits SMEs,* 10 December 2024, https://www.uobgroup.com/asean-insights/articles/port-digitalisation.page (accessed October 12, 2025).

14 Prosertek, *Ports 4.0: How technology is transforming port operations,* https://prosertek.com/blog/ports-4-0-how-technology-is-transforming-port-operations/ (accessed March 15, 2025).

15 Ignacio de la Pena Zarzuelo, 'Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue', *Transport Policy,* 100 (2021), 1-4.

16 Jean Paul Rodrigue, Theo Notteboom, Athanasios Pallis, 'Chapter 3.2: The Digital Transformation of Ports', in *Port Economics, Management and Policy: A comprehensive analysis of the port industry* (Routledge, 2022), https://porteconomicsmanagement.org/pemp/contents/part2/digital-transformation/ (accessed March 15, 2025).

17 TXOne Networks, *Future Cybersecurity Threats in Ports: Protecting Global Trade from Rising Maritime Risks,* January 22, 2024, https://www.txone.com/blog/protecting-global-trade-from-rising-maritime-risks/

18 Risk Intelligence, *The Cybersecurity threat to Ports: Context, assessment, and looking forward, Whitepaper,* May 2021, https://www.riskintelligence.eu/whitepaper-port-cybersecurity (accessed October 12, 2025).

19 Andrew Baskin & Mona Swoboda, 'Automated Port Operations: The Future of Port Governance', Chapter 8, in Tafsir Matin Johansson, Dimitrios Dalaklis, Jonatan Echebarria Fernández, Aspasia Pastra, Mitchell Lennan (eds), *Smart Ports and Robotic Systems, Navigating the Waves of Techno-Regulation and Governance* (Palgrave Macmillan, 2023).

20 Jean Paul Rodrigue, Theo Notteboom, Athanasios Pallis, 'Fully and Semi Automated Container Terminals', in *Port Economics, Management and Policy: A comprehensive analysis of the port industry* (Routledge, 2022), https://porteconomicsmanagement.org/pemp/contents/part3/terminal-automation/fully-semi-automated-container-terminals-total-hectares/ (accessed March 19, 2025).

21 Gabriel A. Weaver, Brett Feddersen, Lavanya Marla, Dan Wei, Adam Rose, Mark Van Moer, 'Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach', *Transportation Research Part C: Emerging Technologies,* 137 (2022), 103423.

22 LRQA, *Notpetya ransomware attack on Maersk - key learnings (2024),* https://www.lrqa.com/en/insights/articles/notpetya-ransomware-attack-on-maersk-key-learnings/ (accessed October 12, 2025).

23 Philipp Martin Dingeldey, *Port Automation and Cyber Risk in the Shipping Industry,* Centre for International Maritime Security (CIMSEC), 20 December 2017, https://cimsec.org/port-automation-and-cyber-risk-in-the-shipping-industry/ (accessed October 12, 2025).

24 Sangfor Technologies, 'Nagoya Port Cyber Attack by Lockbit Ransomware Results in Cargo Delays', 11 July 2023. https://www.sangfor.com/blog/cybersecurity/nagoya-port-cyber-attack-by-lockbit-ransomware (accessed October 12, 2025).

25 Risk Intelligence, *The Cybersecurity threat to Ports: Context, assessment, and looking forward,* Whitepaper, May 2021, https://www.riskintelligence.eu/whitepaper-port-cybersecurity

26 Ibid.

27 Michael Parrant, 'The Impact of Automation on Cyber Risk', *Aon Insights* (2025), https://aoninsights.com.au/impact-automation-cyber-risk/ (accessed March 18, 2025).

28 'Antwerp incident highlights maritime IT security risk', *Seatrade Maritime News,* 21 October 2013, https://www.seatrade-maritime.com/accidents/antwerp-incident-highlights-maritime-it-security-risk (accessed October 12, 2025).

29 'Ransomware Attack Hits Japan's Biggest Port – how can you prevent such an attack?', *Cydome.io* (n.d.), https://cydome.io/ransomware-attack-hits-japans-biggest-port-how-can-you-prevent-such-an-attack/ (accessed October 12, 2025).

30 Dom Magli, 'DP World Australia hit by cyberattack', *Port Technology,* November 30, 2023, https://www.porttechnology.org/news/dp-world-australia-hit-by-cyber-attack/ (accessed October 12, 2025).

31 'Ransomware Attack at Port of Rijeka', *icsstrive.com,* December 19, 2024, https://icsstrive.com/incident/ransomware-attack-at-port-of-rijeka/ (accessed October 12, 2025).

32 'Media Statement: Update on Cybersecurity Incident', *DP World,* 28 November 2023, https://www.dpworld.com/australia/news/releases/media-statement-update-on-cybersecurity-incident/

33 Nicolas Asfouri, 'New cyber-attacks by pro-Russian hackers hit port and local authority websites', *Belga News Agency,* 8 October 2024, https://www.belganewsagency.eu/new-cyber-attacks-by-pro-russian-hackers-hit-port-and-local-authority-websites

34 Council of Europe (COE), *Convention on Cybercrime,* 23 November 2001, ETS No.185, https://rm.coe.int/1680081561.

35 Ibid.

36 COE, 'Chart of Signatures and Ratifications of Treaty 185', available at https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

37 COE, *Convention on Cybercrime,* Arts 2 – 8.

38 Vibhu Mishra, 'UN General Assembly adopts milestone cybercrime treaty', *UN News* (24 December 2024), https://news.un.org/en/story/2024/12/1158521.

39 "United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes", in: UNGA, *Countering the use of information and communications technologies for criminal purposes,* Report of the Third Committee, UNGA OR, 79th Session, Agenda item 108, Doc. No. A/79/460 (27 November 2024)., Art. 1.

40 Ibid, Arts 7 – 53.

41 Ibid, Chapter II.

42 *The International Convention for the Safety of Life at Sea,* 1 November 1974, 1184 U.N.T.S 277

43 *International Code for Security of Ships and of Port Facilities,* adopted by the SOLAS Contracting Parties Conference, London, 12 December 2002, Doc.SOLAS/CONF.5/34, Annex 1, part 1.2.

44 Ibid, Annex 1, Part A, 14.1, 15.1 & 16.1

45 Ibid, Annex 1, Part B, 1.7.

46 IMO, *Guidelines on Maritime Cyber Risk Management,* MSC-FAL.1/Circ.3/Rev.2 (7 June 2022), Annex.

47 Ibid.

48 IMO's Maritime Safety Committee, *Maritime Cyber Risk Management in Safety Management System,* Resolution MSC.428(98) (16 June 2017).

49 See ISO/IEC 27001 Information Security Management Systems. Current Edition: ISO/IEC 27001:2022 available at https://www.iso.org/standard/27001#lifecycle.

50 IAPH, *Cybersecurity Guidelines for Ports and Port Facilities,* Version 1.0, Sustainable World Ports (2 July 2021), https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf

51 Ibid.

52 IAPH, *Cyber Resilience Guidelines for emerging Technologies in the Maritime Supply Chain,* Jun 18, 2025, https://issuu.com/portsandharbors/docs/iaph_cyber_resilience_guidelines_for_emerging_tech (accessed October 13, 2025).

53 'IAPH releases cyber security guidelines for new port technologies', June 24, 2025, https://safety4sea.com/iaph-releases-cyber-security-guidelines-for-new-port-technologies/ (accessed October 13, 2025).

54 National Institute of Standards and Technology (NIST), *Framework for improving critical infrastructure cybersecurity, Version 1.0,* February 12, 2014, https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

55 American National Standards Institute (ANSI), 'NIST releases cybersecurity framework version 2.0', *ANSI.org* (26 February 2024), https://www.ansi.org/standards-news/all-news/2024/02/2-26-24-nist-releases-cybersecurity-framework-version-2.

56 ASEAN, *CIIP Guidelines Ver.3, the 9th ASEAN-Japan Information Security Policy Meeting, 20 October 2016,* https://asean.org/wp-content/uploads/2012/05/01-CIIP-Guidelines-Ver3.0.pdf; see National Center of Incident Readiness and Strategy for Cybersecurity (NISC), 'Asean – Japan Collaboration on Information Security' (2015), https://www.nisc.go.jp/eng/fw_top.html.

57 Ibid, s1-1 (a) & ss 2-1 – 2-9.

58 ASEAN, *ASEAN Data Management Framework: Data Governance and Protection throughout the Data Lifecycle,* endorsed by the ASEAN Digital Senior Officials Meeting, January 2021, https://asean.org/wp-content/uploads/2021/08/ASEAN-Data-Management-Framework.pdf

59 Ibid.

60 ASEAN, *ASEAN Digital Master Plan 2025,* https://asean.org/wp-content/uploads/2021/08/ASEAN-Digital-Masterplan-2025.pdf; adopted at the 1st ASEAN Digital Minister Meeting Joint Media Statement, 21 – 22 January 2021 via videoconference under Malaysian chair.

61 Ibid. at 22.

62 L. Chang, 'Cybercrime and Cyber security in ASEAN', in J. Lieu, M. Travers & L. Y.C. Chang (eds) *Comparative Criminology in Asia* (Charm: Springer, 2017), 135-148 at 9.

63 ASEAN, 'Joint Media Statement of the 6th ASEAN Telecommunications and IT Ministers Meeting', Brunei Darussalam, 16 – 18 September 2006, s11, https://asean.org/joint-media-statement-sixth-asean-telecommunications-and-it-ministers-meeting-brunei-darussalam/ See also 15th Iteration of Asean Cert Incidents Drill Tests Certs' Preparedness Against Opportunistic Covid-19-Related Campaigns, October 8, 2020, available at *https://www.csa.gov.sg/en/News/News-Articles/15th-asean-cert-incident-drill.*

64 P. Tanakasempipat, *Southeast Asian cyber security center opens in Thailand,* September 14, 2018, Reuters, available at https://www.reuters.com/article/us-asean-cyber-idUSKCN1LU1G0.

65 G. Domiguez, 'ASEAN sets up regional office for cybersecurity cooperation', July 18, 2023, *Japan Times,* https://www.japantimes.co.jp/news/2023/07/18/asia-pacific/asean-cyberattacks-operations-center/; ACICE, 'About Us', available at https://www.acice-asean.org/aboutacice/.

66 'The 5 Biggest Ports in Southeast Asia', January 22, 2020, https://www.porttechnology.org/news/the-5-biggest-ports-in-southeast-asia/ (accessed October 12, 2025).

67 The MPA was established by the Maritime and Port Authority of Singapore Act 1996 on 2 February 1996 with the mission to develop Singapore as a premier global hub port and international maritime center as well as to advance and safeguard Singapore's strategic maritime interest. https://www.sgdi.gov.sg/ministries/mot/statutoryboards/mpa (accessed October 12, 2025).

68 PSA Singapore, https://www.singaporepsa.com/ (accessed October 12, 2025).

69 2025 another record year for S'pore's port as containers handled, vessel arrivals hit new highs https://www.straitstimes.com/singapore/transport/2025-another-record-year-for-spores-port-as-containers-handled-vessel-arrivals-hit-new-highs.

70 World Ports Sustainability Program, 'MPA Singapore – Digital Port Ecosystem', 2020, https://sustainableworldports.org/project/mpa-singapore-digital-port-ecosystem/ (accessed October 12, 2025).

71 The requirement under the Convention on Facilitation of International Maritime Traffic (FAL) requires Governments to use a single digital platform or "Maritime Single Window" to share and exchange information with ships when they call at ports, since 1 January 2024. IMO, *Maritime Single Window - advancing digitalization in shipping,* 31 January 2024, https://www.imo.org/en/mediacentre/pressbriefings/pages/maritime-single-window-advancing-digitalization-in-shipping.aspx (accessed October 12, 2025).

72 Maritime and Port Authority of Singapore (MPA), 'Single Window Port Clearance, Digital Port@SG', https://www.mpa.gov.sg/finance-e-services/digitalport@sg (accessed March 18, 2025).

73 Ibid.

74 'World's largest automated terminal: PSA Tuas Port pioneering automation transformation with event-driven architecture', *Seatrade Maritime News,* 14 February 2024, https://www.seatrade-maritime.com/terminals/world-s-largest-automated-terminal-psa-tuas-port-pioneering-automation-transformation-with-event-driven-architecture (accessed October 12, 2025).

75 Singapore Cybersecurity Agency, 'Information on the Cybersecurity Act', 2 April 2025, https://www.csa.gov.sg/legislation/cybersecurity-act (accessed October 12, 2025).

76 Ibid.

[77] Section 2, Cybersecurity Act 2018 (No. 9 of 2018) https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20211231?DocDate=20180312&WholeDoc=1#Sc1-

[78] First Schedule, Essential Services, Cybersecurity Act 2018 (No. 9 of 2018), https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20211231?DocDate=20180312&WholeDoc=1#Sc1-

[79] MPA, *Collective Efforts to Strengthen Maritime Cybersecurity,* 16 Apr 2024, https://www.mpa.gov.sg/media-centre/details/collective-efforts-to-strengthen-maritime-cybersecurity (accessed October 12, 2025).

[80] The Roundtable was established in April 2022 with the aim to strengthen the industry's cybersecurity capabilities and cyber resilience as the sector becomes increasingly digitalised and interconnected.

[81] MPA, 'MPA Collaborates with Microsoft to Boost Innovation, Cybersecurity, Digital, and Green Transformation for Maritime Industry', 30 July 2024, https://www.mpa.gov.sg/media-centre/details/mpa-collaborates-with-microsoft-to-boost-innovation--cybersecurity--digital--and-green-transformation-for-maritime-industry (accessed October 12, 2025).

[82] 'Singapore's MPA launches Maritime Cybersecurity Operations Centre', *Riviera*, 17 May 2019, https://www.rivieramm.com/news-content-hub/news-content-hub/singapores-mpa-launches-maritime-cybersecurity-operations-centre-54661 (accessed October 12, 2025).

[83] MPA, Media Factsheet (Maritime) https://www.mpa.gov.sg/docs/mpalibraries/media-releases/cos-2025_mpa-factsheet_driving-maritime-growth-and-innovation.pdf?sfvrsn=ab672ae4_3

[84] Port of Seattle, Port of Los Angeles, National Ports of Agency of Morocco, Port of Sines, Hamburg Port Authority, Tanger Med Port Authority and Port of Nagoya.

[85] MPA, 'Collective Efforts to Strengthen Maritime Cybersecurity', Media Release, Singapore, 16 April 2024, https://www.mpa.gov.sg/docs/mpalibraries/media-releases/smw-2024---collective-efforts-to-strengthen-maritime-cybersecurity.pdf?sfvrsn=ee064d73_1

[86] ASEAN Ports Association, 'Malaysia', http://apaport.org/country/Malaysia (accessed March 18, 2025).

[87] Development & Administration of Ports, Ministry of Transport Malaysia Official Portal https://www.mot.gov.my/en/maritime/infrastructure/development-administration-of-ports (accessed March 18, 2025).

[88] Suhara Mohd Sidik, 'Regulatory Issues in Port Business and Operations in Malaysia', *Azmi & Associates,* https://www.azmilaw.com/insights/regulatory-issues-in-port-business-and-operations-in-malaysia/ (accessed March 18, 2025).

[89] Ibid.

[90] 'Westports Malaysia's Remote Physical-Check System wins award for infrastructure technology in cargo handling', *Singapore Business Review,* https://sbr.com.sg/co-written-partner/event-news/westports-malaysias-remote-physical-check-system-wins-award-infrastructure-technology-in-cargo-handling (accessed October 12, 2025).

[91] Malaysian Investment Development Authority, 'Navigating the Future: Enhancing Malaysia's Port Development and Logistics Performance with Digitalisation' (2025), https://www.mida.gov.my/navigating-the-future-enhancing-malaysias-port-development-and-logistics-performance-with-digitalisation/ (accessed March 18, 2025).

[92] Margherita Bruno, 'Port Tanjung Pelepas turns to AI-powered management system', *Port Technology,* June 26, 2022. https://www.porttechnology.org/news/malaysian-ptp-turns-to-ai-powered-management-system/

[93] Kiran Jacobs, 'PTP Charts New Course With Digital Makeover', *The Edge Malaysia,* 28 August 2023, https://theedgemalaysia.com/node/680193?utm_source=Newswav&utm_medium=Website

[94] Syed Rakin Rahman, 'Port of Tanjung Pelepas launches truck optimisation tool', *Port Technology,* March 12, 2025, https://www.porttechnology.org/news/port-of-tanjung-pelepas-launches-truck-optimisation-tool/

[95] Jacobs, 'PTP Charts New Course'.

[96] Cyber Security Act 2024 [Act854], Section 4, Date of Royal Assent 18 June 2024; Date of publication in the Gazette 26 June 2024.

[97] 'Malaysia's Premiere Logistics Hub: Port of Tanjung Pelepas', *Port Technology,* https://www.porttechnology.org/technical-papers/malaysias-premiere-logistics-hub-port-of-tanjung-of-pelepas/ (accessed October 12, 2025).

[98] 'Biggest ports in Indonesia for international trade', *InCorp*, May 16, 2024, https://indonesia.incorp.asia/blogs/international-ports-in-indonesia/ (accessed October 12, 2025).

[99] Takashima Minoru, 'The current situation and future initiatives of Yanjung Priok Port', *JTTRI AIRO*, https://www.jttri-airo.org/en/dll.php?id=30&s=pdf1&t=repo (accessed March 19, 2025).

[100] Ibid.

[101] Menteri Perhunungan, Republik Indonesia, Peraturan Menteri Perhubungan Republik Indonesia Nomor OM 15 Tahun 2023.

[102] Nofie Iman, Muhammad Tafdhil Amanda and Jovita Agenla, 'Digital Transformation for Maritime Logistics Capabilities Improvement: Cases in Indonesia', *Marine Economic and Management 5*(2) (2022).

[103] International Trade Administration, 'Indonesia Infrastructure Smart Port Development', 15 October 2024, https://www.trade.gov/market-intelligence/indonesia-infrastructure-smart-port-development (accessed October 12, 2025).

[104] 'Minister aims for 149 green, smart ports by 2024', ANTARA, December 28, 2022, https://en.antaranews.com/news/267684/minister-aims-for-149-green-smart-ports-by-2024 (accessed October 12, 2025).

[105] International Trade Administration, 'Indonesia Infrastructure Smart Port Development'.

[106] Ibid.

107 Dani Rusli Utama, Mohammad Hamsal, Sri Bramantoro Abdinagoro, Rano Kartono Rahim, 'Developing a digital transformation maturity model for port assessment in archipelago countries: The Indonesian case', *Transportation Research Interdisciplinary Perspectives,* 26 (2024), 101146.

108 Ibid.

109 Mochamad Azhar, 'Indonesia drafting long-pending Cybersecurity Bill, says Minister', *Gov Insider,* 05 March 2025), https://govinsider.asia/intl-en/article/indonesia-drafting-long-pending-cybersecurity-bill-says-minister (accessed October 12, 2025).

110 Ibid.

111 SSEK Law Firm, *Fortifying Indonesia's Cyber Defenses: New Regulations for National Security and Crisis Management,* 20 May 2024, https://ssek.com/blog/fortifying-indonesias-cyber-defenses-new-regulations-for-national-security-and-crisis-management/ (accessed October 12, 2025).

112 Erik Purnama Putra, 'Kemenhub Dorong Pengamanan Pelabuhan Terkait Cyber Security', *Republika*, 18 May 2024, https://news.republika.co.id/berita/sdoa56484/kemenhub-dorong-pengamanan-pelabuhan-terkait-cyber-security (accessed October 12, 2025).

113 Bayu Jagadsea, 'Perdana, Kemenhub Gelar Joint Exercise Port Facilities Cyber Attack & Traffic Impact', Maritim News, https://maritimnews.com/2024/02/perdana-kemenhub-gelar-joint-exercise-port-facilities-cyber-attack-traffict-impact/amp/ (accessed October 12, 2025).

114 Fortinet, *What Is Cyber Insurance? Why Is It Important?* (2025), https://www.fortinet.com/resources/cyberglossary/cyber-insurance.

115 Federation of European Private Port Companies and Terminals (FEPORT), 'ENISA releases report about cybersecurity in ports', 26 November 2019, https://www.feport.eu/media-corner/news/general-news/25-news-posts-2019/540-enisa-releases-report-about-cybersecurity-in-ports.

116 US Coast Guard News, Department of Homeland Security, Final Rule: Cybersecurity in the Marine Transportation System – Implementation Timeline, 16 July 2025. https://www.news.uscg.mil/maritime-commons/Article/4247529/final-rule-cybersecurity-in-the-marine transportation-system-implementation-tim/

117 The Institution of Engineering and Technology, *Cyber Security for Ports and Port Systems* (UK Department of Transport, 2016), https://assets.publishing.service.gov.uk/media/5e284eefe5274a6c3ee68fcd/cyber-security-for-ports-and-port-systems-code-of-practice.pdf

118 Vu Hai Dang & Su Wai Mon (2023), 'Improving Maritime Cybersecurity in Southeast Asia: Suggestions for Further Action by ASEAN', *Asia-Pacific Journal of Ocean Law and Policy 8* (2023): 329-335 (see 332).

BLUE
SECURITY