MOBILITY AND TRANSPORT CONNECTIVITY SERIES

DECEMBER 2020

ACCELERATING DIGITALIZATION

Critical Actions to Strengthen the Resilience of the Maritime Supply Chain

WORLD BANK GROUP

IAPH International Association of Ports and Harbors

WPSP WORLD PORTS SUSTAINABILITY PROGRAM

MOBILITY AND TRANSPORT CONNECTIVITY IS A SERIES PRODUCED BY THE TRANSPORT GLOBAL PRACTICE OF THE WORLD BANK. THE WORKS IN THIS SERIES GATHER EVIDENCE AND PROMOTE INNOVATION AND GOOD PRACTICES RELATING TO THE DEVELOPMENT CHALLENGES ADDRESSED IN TRANSPORT OPERATIONS AND ANALYTICAL AND ADVISORY SERVICES.

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

Contents

Figures

Boxes

Tables

Acknowledgments

This technical report was prepared by a joint team of representatives from the Transport Global Practice of the World Bank and the World Ports Sustainability Program (WPSP) of the International Association of Ports and Harbors (IAPH). The World Bank team was led by Richard Martin Humphreys (Global Lead for Transport Connectivity and Regional Integration, and Lead Transport Economist, ITRGK) and Ninan Oommen Biju (Senior Port and Maritime Transport Specialist, IEAT1), with the support of Hua Tan (Senior Transport Specialist, IEAT2), Tong Zhu (Consultant, IEAT2), and Sandra Sargent (Senior Digital Development Specialist, IDD01). The International Association of Ports and Harbors Team was led by Dr. Patrick Verhoeven, Managing Director of the International Association of Ports and Harbors and Coordinator, World Ports Sustainability Program, and Pascal Ollivier, President of Maritime Street and Chairman, IAPH Data Collaboration Committee.

The lead authors thank the following for their substantive contributions to the preparation of this report: Tom Monballiu, International Community Relations Manager, Port of Antwerp; Piet Opstaele, Innovation Enablement Manager, Port of Antwerp; Bob Spanoghe, Innovation Platform Manager, Port of Antwerp; Julian Abril Garcia, Head, Facilitation, International Maritime Organization; Martina Fontanet Sole, Technical Officer, International Maritime Organization[1]; Richard Morton, Secretary General, International Port Community System Association; Jaume Bagot, Business Process Improvement Manager, Port de Barcelona; Eric Caris, Director of Marketing, Port of Los Angeles; Lance Kaneshiro, Chief Information Officer, Port of Los Angeles; Ben van Scherpenzeel, Chairman, International Taskforce Port Call Optimization; Franz Van Zoelen, Special Projects—Head Legal Emeritus, Port of Rotterdam, Legal Counselor of IAPH, and Chairman of IAPH Legal Committee; Mees van der Wiel, Business Consultant, Strategy & Innovation, Portbase; Max J. Bobys, Vice President, Hudson Cyber; Troy Vest, Vice President, Hudson Trident; Andrew Baskin, Vice President, Global Trade Policy, Hudson Analytix; Lee Eung-hyuk, Director of Marketing &International Affairs, Busan Port Authority; Dr. Phanthian Zuesongdham, Head of Digital and Business Transformation, and Head of smartPORT Programme Management, Hamburg Port Authority; Heng Huang, General Manager, and Jue Chen, Business Planning Manager, both of Shanghai Harbor e-Logistics Software Company, Ltd., a subsidiary of Shanghai International Port Group; and Victor Shieh, Communications Partner, World Ports Sustainable Program, International Association of Ports and Harbors.

We also extend particular thanks to the following for their comments on the report draft: Gylfi Palsson (Lead Transport Specialist, IAET2); Yin Yin Lam (Senior Transport Specialist, IAET1); Hagai Mei Zahav (Consultant, IDD01); and Jorge Duran, Chief of Section, Inter-American Committee on Ports, Organization of American States.

The lead authors and report contributors extend special thanks to Ms. Tessa Major, Chair, IAPH COVID-19 Task Force, and Director, International Business & Innovation, Port of Açu, for her leadership of the task force and her unwavering support in this joint effort between the World Bank and IAPH.

1 The views expressed herein are those of the author(s) and do not necessarily reflect the views of IMO.

Abbreviations and Acronyms

AI	artificial intelligence
AR	augmented reality
API	application programming interface
APICA	Antwerp Port Information and Control Assistant
BAPLIE	bayplan/stowage plan occupied and empty locations message
BIMCO	Baltic and International Maritime Council
B2B	business-to-business
B2G	business-to-government
CCTV	closed-circuit television
COVID-19	Coronavirus Disease 2019
CRC	Cyber Resilience Center
DBI	Doing Business index
EDI	electronic data interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EGDH	Expert Group on Data Harmonization
ENISA	European Union Agency for Cybersecurity
FAL	Convention on Facilitation of International Maritime Traffic
FONASBA	Federation of National Associations of Ship Brokers and Agents
GCI	Global Competitiveness Index
GDP	gross domestic product
GDPR	General Data Protection Regulation
IALA	International Association of Marine Aids to Navigation and Lighthouse Authorities
IAPH	International Association of Ports and Harbors
ICC	International Chamber of Commerce
ICHCA	International Cargo Handling Coordination Association
ICS	International Chamber of Shipping
IFTSAI	international forwarding and transport schedule and availability information message
IHMA	International Harbor Masters' Association
IHO	International Hydrographic Organization
ILO	International Labour Organization
IMO	International Maritime Organization
IMPA	International Maritime Pilot's Association
IPCSA	International Port Community Systems Association
ISSA	International Shipsuppliers & Services Association
ITPCO	International Taskforce Port Call Optimization
ICS	International Chamber of Shipping
IOT	internet of things
ISM	international safety management
ISPS	International Ship and Port Facility Security
ISO	International Organization for Standardization
JIT	just-in-time
LPI	Logistics Performance Index
MSC	Maritime Safety Committee
MSW	maritime single window

NIST	National institute of Standards and Technology
NTFC	national trade facilitation committee
NSW	national single window
OT	operational technology
PCO	port call optimization
PCS	port community system
PFSA	port facility security assessment
PFSP	port facility security plan
PFSO	port facility security officer
PIM	port information manual
PMS	port management system
PMIS	port management information system
SCADA	supervisory control and data acquisition
SOLAS	International Convention for the Safety of Life at Sea
TEU	twenty-foot equivalent unit
TOS	terminal operating system
UAS	unmanned aerial systems
UNCTAD	United Nations Conference on Trade and Development
UNECE	United Nations Economic Commission for Europe
VBS	vehicle booking system
VR	virtual reality
VTMS	vessel traffic management information system
WCO	World Customs Organization
WTO	World Trade Organization

Glossary

CYBERSECURITY

Cybersecurity encompasses the capability to protect or defend against unauthorized access to or use of cyberspace from cyberattacks. Cybersecurity includes the collective measures implemented to defend a computer or computer-enabled system against cyber-enabled threats, such as hackers, hacktivists, foreign intelligence services, and organized criminal syndicates, among others.

DIGITAL HEALTH SECURITY

Digital health security involves the digital capability to protect workers at sites of critical infrastructure. Digital health security consists of the necessary digital measures to ensure business continuity and protect port workers from potential infection during the COVID-19 pandemic such as enforcing social distancing and temperature control of port workers.

DIGITAL PORT SECURITY

Digital port security involves the digital capability to protect ports as critical infrastructure vital to economy and security. Digital port security consists of the need for global control of assets, goods, and people through digital technologies.

PORT CALL OPTIMIZATION (PCO)

Port call optimization, or PCO, is about optimizing speed, draught, and port stay, leading to lower costs, cleaner environment, more reliability, and safety for shipping, terminals and ports.

MARITIME SINGLE WINDOW (MSW)

A maritime single window, or MSW, is a one-stop service environment that covers maritime and port administrative procedures, such as port entry and departure declaration, notice of security reports, and other related information between private sectors and public authorities in the port. In other words, an MSW is a single window in the scope of maritime and port fields, and would exclude the interactions related to the clearance of the consignment itself.

PORT COMMUNITY SYSTEM (PCS)

A port community system, or PCS, is a neutral and open electronic platform enabling intelligent and secure exchange of information between public and private stakeholders in order to improve the competitive position of the sea and air ports' communities. The PCS is intended to optimize, manage, and automate port and logistics processes through a single submission of data and by connecting transport and logistics chains.

PORT MANAGEMENT SYSTEM (PMS)

A port management system, or PMS, enables the port authority to control traffic and manage port infrastructure, such as port calls, dues, journal, incidents, waste, dangerous goods, planner, cargo, inspections, permits, services, security, and assets.

SINGLE WINDOW

In the annex to the Convention on Facilitation of International Maritime Traffic (the FAL Convention), a single window, is defined as a facility that allows submission of standardized information covered by the convention to a single-entry point. The facility is generally understood to be based on electronic data transmission and relies on system software to distribute the data submitted to the receivers in accordance with the system rules and user agreements. The literal definition of single window allows for any type of data transmission that employs a single-entry point and avoids duplication.

United Nations Economic Commission for Europe (UNECE) Recommendation N°.331 defines a "single window" as an electronic facility providing trade facilitation measures that allows parties involved in trade and transport to lodge standardized information and documents with a single-entry point to fulfil all import, export, and transit-related regulatory requirements. Individual data elements should only be submitted once electronically.

NOTE

1. To access UNECE Recommendation No. 33 online, go to: https://www.unece.org/fileadmin/DAM/cefact/recommendations/rec33/rec33_trd352e.pdf.

SMART PORT

A smart port is an automated port that uses nascent technologies such as big data, internet of things (IoT), blockchain solutions, and other smart technology-based methods to improve performance and economic competitiveness. With these technologies, smart ports can also improve environmental sustainability. In an ideal smart port, processes would be automated and connected via IoT.

TERMINAL OPERATING SYSTEM (TOS)

Employed in maritime, waterway, rail-to-rail, and intermodal rail terminal operations, a terminal operating system, or TOS, provides visibility, control, optimization, scheduling, planning, analytics, and automated handling of maritime containers, rail containers, and break bulk.

VESSEL TRAFFIC MANAGEMENT INFORMATION SYSTEM (VTMIS)

A vessel traffic management information system, or VTMIS, integrates and interconnects all the relevant assets to manage maritime operations safely and securely. This includes management of maritime operations from marine environmental protection to traffic management, law enforcement, and security at sea.

Forewords

I am very pleased to introduce this transport-focused technical report on "accelerating digitalization," conceived as a follow-up to a policy statement issued in early June 2020—in the wake of the COVID-19 pandemic—by a number of port and maritime industry organizations. In that original statement, the signatories jointly called upon international and intergovernmental organizations, governments and industry stakeholders concerned with maritime trade and logistics to come together and accelerate the pace of digitalization so that port communities across the world can at minimum offer a basic package of electronic commerce and data exchange. The statement listed nine priority areas, ranging from port call optimization to cybersecurity, and was endorsed by the secretary general of the International Maritime Organization.

The COVID-19 crisis has emphasized the critical role of seaports in keeping supply chains moving and economies functioning across the world. A great variety of business and government actors interact in port communities to ensure multimodal flows of vital medical and food supplies, critical agricultural products, energy streams, and other goods and services reach their intended destinations in time. Their interactions comprise physical interactions, such as cargo handling operations, vessel-related services, and multimodal transfers, along with exchanges of data that facilitate clearance of cargo between jurisdictions.

When it comes to digitalization, the COVID-19 crisis has painfully demonstrated the heterogeneous landscape that currently exists across ports worldwide. While some port communities have seized the opportunities found in the Fourth Industrial Revolution and have developed into full-fledged "smart" ports, many others have barely grasped the essentials of digitalization and continue to struggle with larger reliance on personal interaction and paper-based transactions as the norms for shipboard, ship-to-shore interface, and shore-to-hinterland based exchanges.

In producing this report, the authors reveal a keen willingness to action the message of the initial policy statement in practice, outlining in concrete terms short- and medium-term measures to accelerate digitalization that will improve resilience and efficiency in port communities around the world. The report is also intended to facilitate the necessary policy reform in these areas, as digitalization is not just a matter of technology but, more importantly, of change management, data collaboration, and political commitment.

I am most grateful to the team at the World Bank and every port expert who contributed to this paper. Although a wonderful example of a collaborative effort between industry partners, its timely conception is in no small part due to the efforts of long-standing IAPH member Pascal Ollivier, president of Maritime Street, an authority in the field of digital trade logistics. The relentless enthusiasm and energy of Pascal ensured that this insightful report was produced in a record time of just two months. It can now start its journey around the world and pave the way for the next stages in our global effort to help the port and maritime industry embrace the digital era.

Dr. Patrick Verhoeven

Managing Director, International Association of Ports and Harbors
Coordinator, World Ports Sustainability Program

The *World Development Report 2016: Digital Dividends* underlined how digital technology creates opportunities to accelerate growth, generate jobs, and improve services. However, in some sectors these opportunities are often missed, or at the very least delayed, because firms and public authorities are either protected from innovation, or face real barriers to implementation in the form of institutional or regulatory obstacles, and insufficient human capital or resources to implement the changes. The risks facing these sectors and countries include slower economic growth, lower employment, poorer services, and higher trade costs.

The digital revolution has emerged in the past decade as one of the main drivers of change in the port and maritime sector, promoting a high level of integration between devices, agents, and activities. Together with the increased connectivity between ports, it has created a new ecosystem in the industry—one where being on the outside presents a significant disadvantage for ports and countries.

The COVID-19 pandemic has underlined the importance of these changes, with one of the early lessons being the need to ensure business continuity and improving the resilience of critical supply lines, such as the maritime gateways and associated logistical chains. Maritime transport carries 90 percent of the global merchandise trade, and impediments to ports' logistical chains will have tangible repercussions for port hinterlands and their populations. In the short term, these impediments will likely drive shortages of essential goods and higher prices; in the medium to longer term, they could result in slower economic growth, lower employment, and higher trade costs.

However, growing digital integration is not without risk: Cybersecurity is now one of the major challenges facing the maritime industry. Policymakers need to work with the private sector to ensure critical infrastructure is adequately protected, while continuing to help achieve the full benefits of new technologies in a sector where the digital transition has been uneven across countries.

This World Bank technical report, produced in collaboration with the International Association of Ports and Harbors, the World Ports Sustainability Program, and their members, is both timely and welcome and will hopefully stimulate a dialogue among key stakeholders and move this essential agenda forward. Digital technologies will enable the competitive business environments, increased accountability, and better education and skills-development systems that will create the maritime jobs of the future. The World Bank Group stands ready to help countries pursue these priorities.

Ms. Boutheina Guermazi

Director, Digital Development
The World Bank

Executive Summary

1. ***The COVID-19 pandemic has upended lives and brought major disruption to economic activity across the world, precipitating an unprecedented global health and economic crisis.*** Although too early for a full assessment of the impact of the pandemic, it is clear that COVID-19 has brought severe hardship, especially to landlocked and least developed countries, and poor and vulnerable communities. The challenges include inter alia (Latin for "among other things") food insecurity, lack of medical supplies, loss of income and livelihood, difficulties in applying sanitary and physical distancing measures, a looming debt crisis as well as related political and security risks. Vulnerable sectors (for example, tourism, the oil and gas industry, maritime, air and road transport, freight forwarding, logistics, and wholesale and retail sectors) were hit especially hard; some might not recover.

COVID-19 has brought severe hardship to economic activity across the world

2. ***One of the key lessons learned early in the pandemic was the need to ensure business continuity of the critical supply lines, notably the maritime gateways, and the associated logistical chains.*** Maritime transport carries 90 percent of all merchandise trade, and as such any impediment to the maritime logistical chains, results in tangible repercussions for countries served by the port, and their respective populations. While to a greater or lesser extent, the initial challenge has been met and overcome in some countries, experience so far and the risk of subsequent waves underlines the urgent need to improve the resilience of the maritime sector, through accelerating the digitalization of maritime trade and logistics, which will automate trading across borders and reduce traditional human interaction and paper-based transactions.

The digital revolution has emerged in the past decade as one of the main drivers of change in the port and maritime sector

3. ***However, the maritime ports are also just one node in a complex logistical chain involving a number of interactions; digitization is vital to improving the competitiveness of that chain.*** The digital revolution has emerged in the past decade as one of the main drivers of change in the port and maritime sector, and requires a high level of integration between devices, agents, and activities. This, together with the increased connectivity between ports, has created a new ecosystem in the industry—one where being on the outside is a significant disadvantage for ports and countries. It is vital that maritime ports improve their position in respect of technological innovation and integration, both to ensure or improve their competitiveness, but also to reduce the cost of international trade for their respective hosts and hinterland. Because maritime transport carries 90 percent of

global merchandise trade, impediments to ports' logistical chains will have tangible repercussions. In the short term, these impediments will likely drive shortages of essential goods and higher prices; in the medium to longer term, they could result in slower economic growth, lower employment, and higher trade costs.

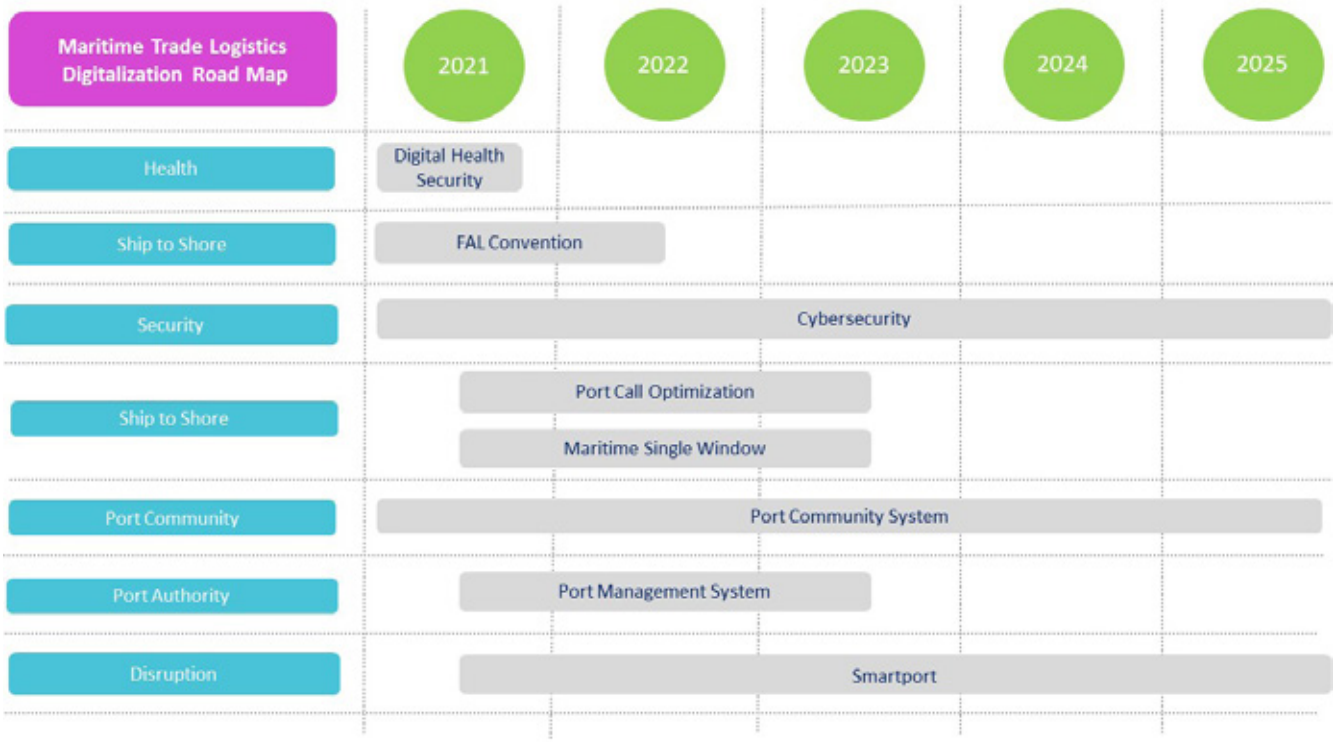
The digital revolution has emerged in the past decade as one of the main drivers of change in the port and maritime sector

4. ***A number of global organizations, such as UNCTAD, UNECE, WCO, WTO, and IMO have been advocating the accelerated digitalization of cross-border processes and documentation.*** The objectives have been to not only keep trade flowing in current and future events, but also protect frontline workers at sea and on land while enabling remote working, with contactless electronic solutions replacing paper documents. Unfortunately, as of November 2020, only 49 of the 174 member states of the International Maritime Organization (IMO) possess functioning port community systems (PCSs)—with higher income countries making up the majority of those that do have port community systems in place. The delay in introduction poses a risk to the business continuity during subsequent waves of the pandemic, along with a further risk over a slightly longer period, which would result from the development of a two-tier system, with laggards facing increased costs for the import and export of merchandise trade.

The objectives have been to not only keep trade flowing in current and future events, but also protect frontline workers at sea, but also protect frontline workers at sea and on land while enabling remote working

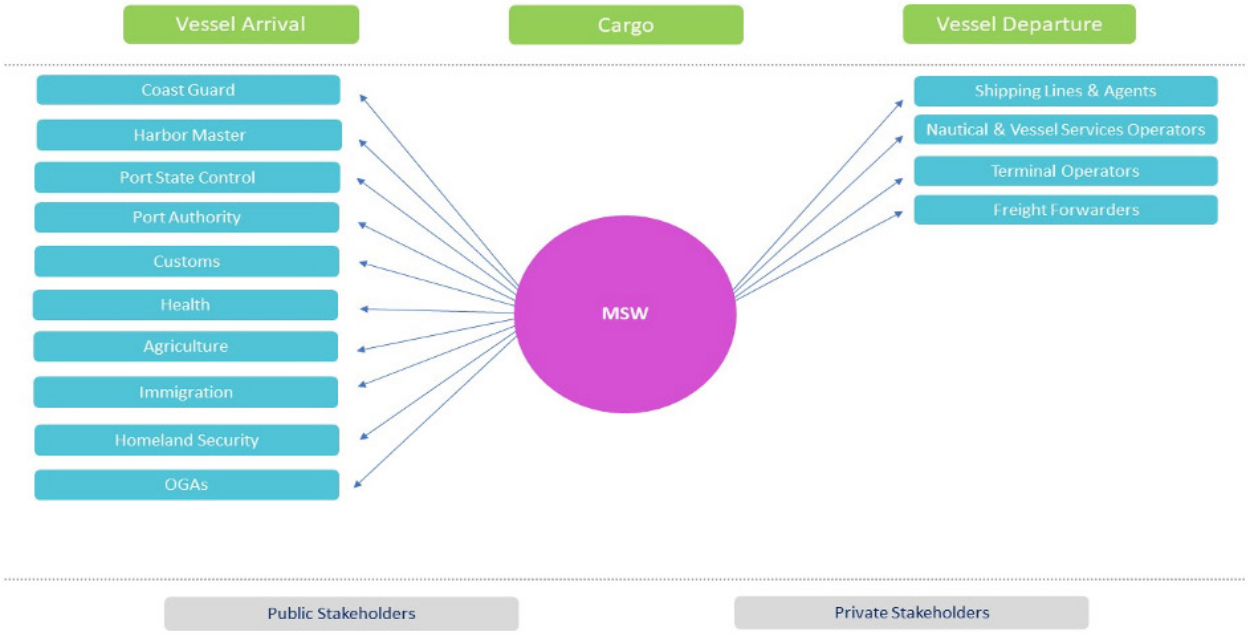
5. ***This report highlights the immediate, short-, and medium-term measures considered necessary to strengthen the resilience of the maritime and logistics sector, to build back better, and more importantly ensure countries realize the significant potential efficiency gains of digitization.*** Figure E.1 provides a schematic of the proposed road map and approximate timeline toward improving the digitization of the maritime logistic chain for any country. The figure illustrates the necessary immediate, short-, and medium-term measures, and a generic timeline for their introduction. The road map encompasses the emergency measures on digital health security monitoring and the establishment of an intergovernmental agencies crisis management center to protect crews, port workers, and passengers from cruises and ferries in the "new normal" by enforcing social distancing and temperature control of port workers.

Figure E.1. Maritime Trade Logistics: Digitalization Road Map



6. ***The immediate measures are followed by, but could also be in parallel to, the short-term measures to meet the mandatory requirements, as defined in the IMO's Facilitation (FAL) Convention (IMO 1965).*** The FAL Convention seeks to support transmission, receipt, and response of information required making the transition to full-fledged maritime single windows (MSWs), for example: the arrival, stay, and departure of ships, persons, and cargo via electronic data exchange (see figure E.2). This has been a mandatory requirement for all ports since April 2019, though implementation remains partial at best. The International Association of Ports and Harbors (IAPH) has just launched a survey to ascertain the current status of implementation.

Figure E.2. Maritime Single Window



7. ***However, the standards and data elements need to be harmonized to facilitate the exchange of information ship to port and the interoperability of the electronic systems.*** The need for harmonized maritime-related data and common agreed standards led to the development of the IMO Compendium on Facilitation and Electronic Business.[1] The IMO Compendium is a tool for software developers who design the systems needed to support transmission, receipt, and response via electronic exchange, of information required for arrival, stay and departure of ships, persons, and cargo to or from a port. It consists of an IMO data set and IMO reference data model[2] agreed by the main organizations involved in the development of standards for the electronic exchange of maritime-related information linked to the FAL Convention.

8. ***The IMO Compendium is intended to facilitate the ship-to-port exchange of information and the interoperability of single windows—a key requirement—thereby reducing the administrative burden for ships linked to formalities and ports.*** The IMO Compendium is not conceived to create "new" standards, but rather as a tool to harmonize existing standards and produce guidance for interested parties to automatically map the IMO data set to any of the leading standards and enable companies involved in maritime trade or transport to create software that can communicate no matter the standard on which they are based.

NOTES

1. Find the HTML version of the IMO Compendium online: https://svn.gefeg.com/svn/IMO-Compendium/Current/index.htm.

2. The IMO data set identifies and defines all the data elements related to reporting information requirements, and the IMO reference data model establishes the underlying hierarchical data structure used in electronic data exchange.

9. ***In parallel to the need for ports to meet the FAL Convention requirements, ports also need to initiate the discussion on the nine key data elements related to port call optimization.*** The objective of the latter is to allow ships to optimize speed during the voyage to facilitate a timely arrival at the pilot boarding place, thus securing berths, fairways, and nautical services at the destination ports. This just-in-time (JIT) arrival will also increase port competitiveness.

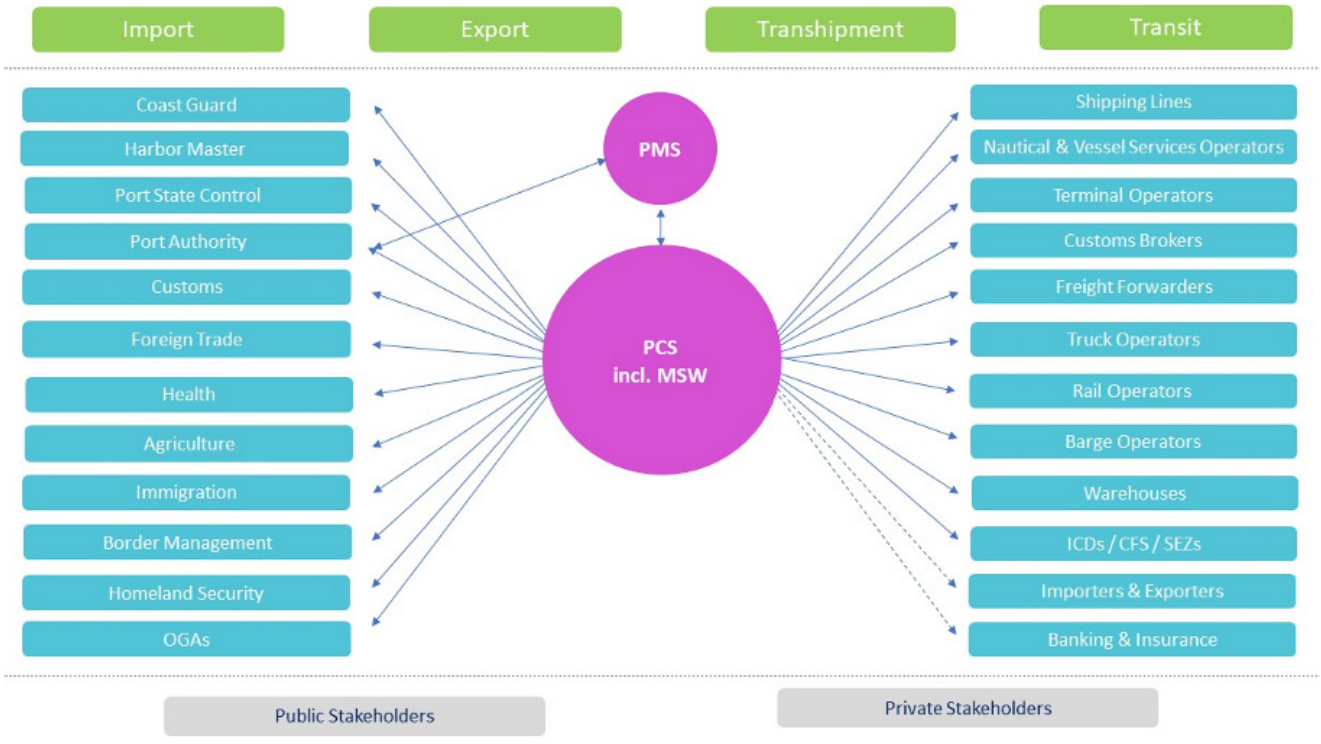
10. ***Equally important, ports must commence the establishment and introduction of a port community system.*** The PCS is a vital platform to optimize, manage, and automate port and logistics processes through a single submission of data in the transport and logistics chain. The coherence between PCS, port management system (PMS), and MSW3 should be ensured in order that the maritime and trade logistics actors can benefit from the digitalization of these processes and associated applications, and that those benefits are realized in a country's international trade costs (figure E.3).

NOTES

3. For further details on the issues surrounding single submission of data in the transport and logistics chain, see the UNECE's Recommendation No. 37: Single Submission Portals, available online: https://www.unece.org/fileadmin/DAM/trade/Publications/ECE_TRADE_447E_CF-Rec37.pdf.

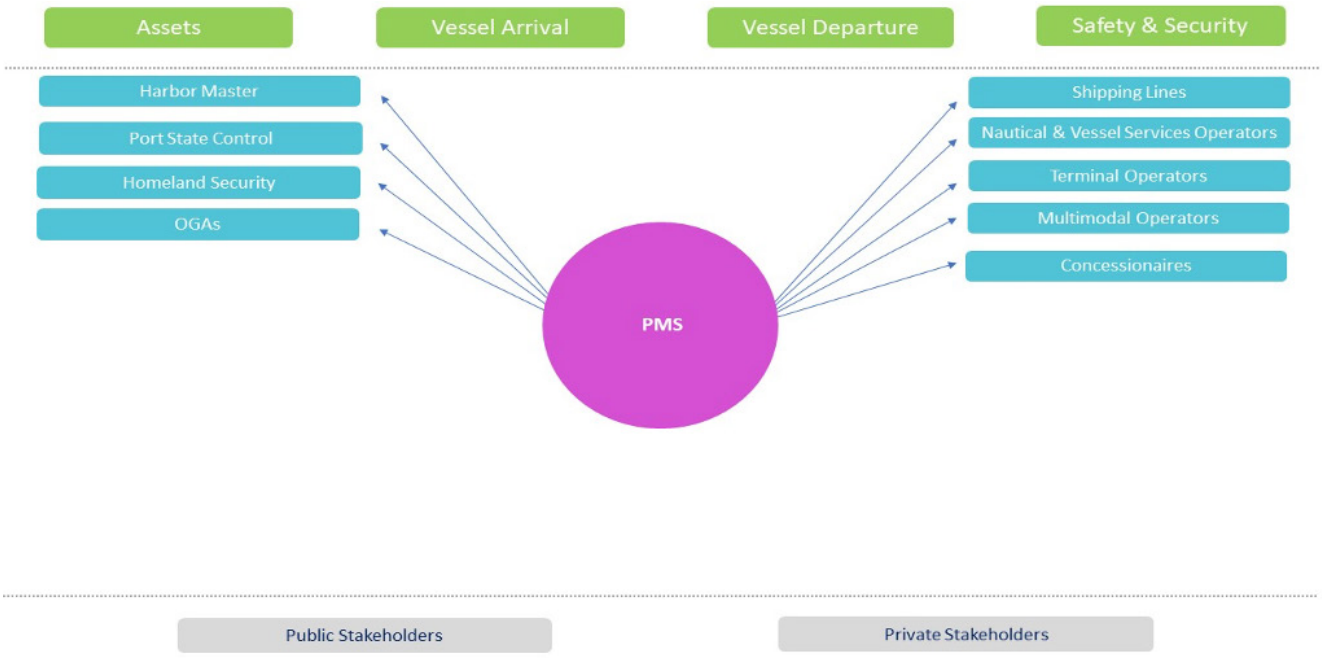
Access the full list of UNECE recommendations for trade facilitation online, here: http://www.unece.org/uncefact/tfrecs.html.

Figure E.3. Port Community System: Optimal Architecture



11. ***In the medium term, every port needs to upgrade to a PMS in order to ensure the full digitalization of all processes related to traffic control and assets management.*** As illustrated in figure E.4, a PMS enables the port authority to control all port traffic through a single digital interface, and manage port infrastructure such as port calls, dues, journal, incidents, waste, dangerous goods, planner, cargo, inspections, permits, services, security, and assets.

Figure E.4. Port Management System



12. ***The last medium-term measure reflects the need for a discussion that will facilitate the movement to the next generation PMS, intended to prepare the transition from cargo hub to digital hub through the smart port concept.*** The latter is defined as an automated port that uses nascent technologies such as artificial intelligence, advanced analytics, internet of things (IoT), fifth-generation technology (5G), autonomous systems, digital twin, blockchain and other distributed ledger solutions as well as other smart technology-based methods to improve performance, economic competitiveness, and environmental sustainability. In an ideal smart port, all processes would be automated and connected via the IoT.

13. ***But increasing the digitization of the maritime logistical chain, while essential, also brings new risks: Between February and May 2020, cyberattacks increased 400 percent in the maritime industry (Captive International 2020)***. In 2017, global container shipping company Maersk and its international port operation wing overcame an aggressive cyberattack—which served as a serious wake-up call. Other attacks have followed and we can be sure that there will be more to come. The risk of a cyberattack has become the top risk for port authorities and the wider port community of stakeholders, necessitating improved cybersecurity at the port community ecosystem level. This report discusses the risks, how a port community should approach mitigating these risks, and provides two such illustrations from the Port of Antwerp (Belgium) and the Port of Los Angeles (California).

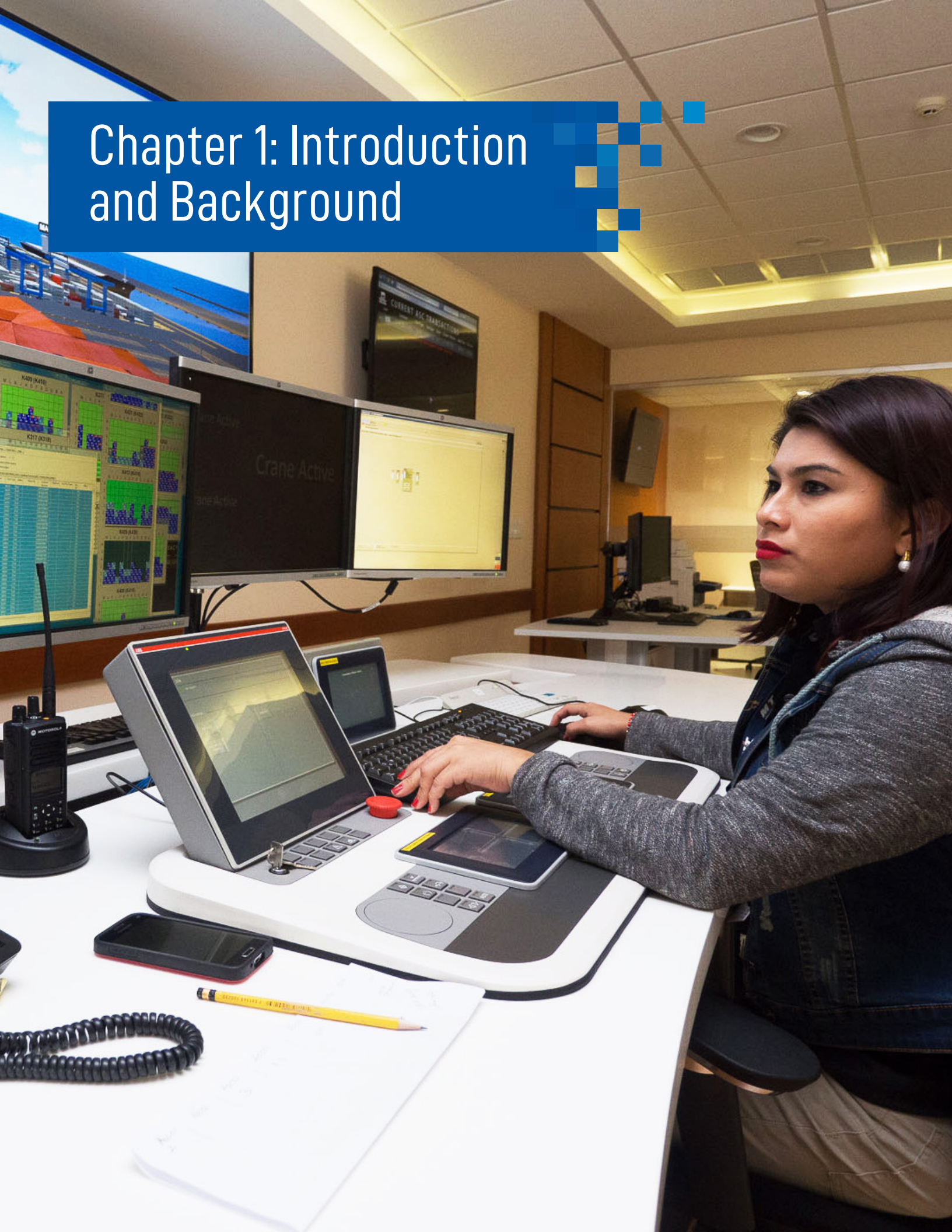
14. ***Finally, this report underlines digitalization as not solely a technological issue, but also as human capital and institutional issues.*** Any move towards increased digitization will require a high level of political commitment, while the establishment must have an appropriate legal, regulatory, and policy framework at the national level, across the different disciplines of the maritime, port, clearance agencies, and the transport and logistics sector. The move toward digitalization will also require improvements in human capital to commission, absorb, and implement the associated demands on stakeholders. Overcoming this challenge will necessitate considerable efforts; therefore, this report proposes establishing a national-level framework to manage the change. This framework encompasses three levels: an interministerial committee, a steering committee, and a business process committee.

REFERENCES

Captive International. 2020. "Maritime Businesses See Fourfold Increase in Cyber Attacks Since February: Astaara." June 23, 2020. https://www.captiveinternational.com/news/maritime-businesses-see-fourfold-increase-in-cyber-attacks-since-february-astaara-3568.

IMO (International Maritime Organization). 1965. Convention on Facilitation of International Maritime Traffic, as amended in 2016. https://www.imo.org/en/About/Conventions/Pages/Convention-on-Facilitation-of-International-Maritime-Traffic-%28FAL%29.aspx.

Chapter 1: Introduction and Background



15. ***The COVID-19 pandemic has upended lives and brought major disruption to economic activity across the world, precipitating an unprecedented global health and economic crisis***. Although too early for a full assessment of the impact of the pandemic, it is clear that COVID-19 has already brought severe hardship, especially to landlocked and least developed countries, and poor and vulnerable communities. The challenges include inter alia (Latin for "among other things") food insecurity, lack of medical supplies, loss of income and livelihood, difficulties in applying sanitary and physical distancing measures, a looming debt crisis as well as related political and security risks. Vulnerable sectors, including tourism, the oil and gas industry, maritime, air and road transport, freight forwarding, logistics, and wholesale and retail sectors, were hit especially hard; some might not recover.

Global pandemic has upended lives and brought major disruption to economic activity across the world

16. ***One of the key lessons learned early in the pandemic was the need to ensure business continuity of the critical supply lines, notably the maritime gateways, and the associated logistical chains.*** Maritime transport carries 90 percent of merchandise trade, and as such any impediment to the maritime logistical chains results in tangible repercussions for countries served by the port and their respective populations. Chapter 2 will outline the essential role of the maritime port in the movement of international trade. While to a greater or lesser extent, the initial challenge has been met and overcome in some countries, experience so far—and the risk of subsequent waves—underlines the urgent need to improve the resilience of the maritime sector, through accelerating the digitalization of maritime trade and logistics.

Maritime transport carries 90 percent of global merchandise trade

17. ***However, the maritime ports are only one node in a complex logistical chain involving a number of interactions; digitization is vital to improving the competitiveness of that chain, and thus in reducing the cost of international trade for countries***. This logistical chain requires the flow of vital medical and food supplies, critical agricultural products, energy streams, and other goods and services. To move efficiently, this flow involves cargo handling operations, vessel-related services and supplies, and integration with road, rail, and the inland water networks, together with the necessary exchange of data to move and clear the consignment across and between jurisdictions. Accordingly, maritime ports must maintain and improve their position in respect to technological innovation and integration, both to ensure or improve their competitiveness and to reduce the cost of international trade for their respective hosts and hinterlands.

Maritime ports must maintain and improve their position in respect to technological innovation and integration

18. ***The digital revolution has emerged in the past decade as one of the main drivers of change in the port and maritime sector.*** By promoting a high level of integration between devices, agents, and activities, and together with the increased connectivity between ports, this digital revolution has created a new ecosystem in the industry—one where being on the outside is a significant disadvantage for ports and countries. Because maritime transport carries 90 percent of the global merchandise trade, impediments to ports' logistical chains will have tangible repercussions for their hinterlands and populations. In the short term, these impediments will likely lead to shortages of essential goods and higher prices; in the medium to longer term, they could drive slower economic growth, lower employment, and higher trade costs.

The digital revolution has emerged as one of the main drivers of change in the port and maritime sector and has created a new ecosystem in the industry

19. ***A number of global organizations, such as UNCTAD, UNECE, WCO, WTO, and IMO, have been advocating the accelerated digitalization of cross-border processes and documentation.*** The objectives have been to not only keep trade flowing during current and future events, but also protect frontline workers at sea and on land while enabling remote working, with contactless electronic solutions replacing paper documents. Unfortunately, as of November 2020, only 49 of the 174 member states of the International Maritime Organization (IMO) possess functioning port community systems (PCSs)—with higher income countries making up the majority of those that do have port community systems in place. The delay in introduction poses a risk to the business continuity during subsequent waves of the pandemic, along with a further risk over a slightly longer period, which would result from the development of a two-tier system, with laggards facing increased costs for the import and export of merchandise trade.

The objectives of accelerated digitalization have been to not only keep trade flowing during current and future events, but also protect frontline workers at sea and on land while enabling remote working

20. ***With the world's attention now focused on preparing for a "new normal," stakeholder collaboration is urgently needed to move this agenda forward.*** This collaboration must encompass intergovernmental organizations, governments, line ministries, and port authorities as well as industry stakeholders in maritime trade and logistics. Working together, they will accelerate the pace of digitalization so that port communities around the world can meet at least the minimum needs in terms of electronic commerce and data exchange—in compliance with all relevant contractual and regulatory obligations—and ensure no port lags behind.

21. ***To initiate this cooperation, a group of international stakeholders issued a recent public call to arms.*** This group—comprising the International Association of Ports and Harbors (IAPH), Baltic and International Maritime Council (BIMCO), the International Cargo Handling Coordination Association (ICHCA), the International Chamber of Shipping (ICS), the International Harbor Masters' Association (IHMA), the International Maritime Pilots' Association (IMPA), the International Port Community Systems Association (IPCSA), the International Shipsuppliers & Services Association (ISSA), the Federation of National Associations of Ship Brokers and Agents (FONASBA), and the PROTECT Group—issued a call to action,[1] highlighting the following priorities:

1. To assess the state of implementation and find ways to enforce the already mandatory requirements defined in the International Maritime Organization's Facilitation (IMO FAL) Convention to support transmission, receipt, and response of information required for making the transition to full-fledged single windows, for example: the arrival, stay, and departure of ships, persons, and cargo, including notifications and declarations for customs, immigration, port, and security authorities via electronic data exchange

2. To ensure harmonization of data standards beyond the IMO FAL Convention to facilitate sharing of port- and berth-related master data for just-in-time (JIT) operation of ships and optimal resource deployment by vessel services and suppliers, logistics providers, and cargo handling and clearance, thereby saving energy, improving safety as well as cutting costs and emissions. This can be achieved through use of the supply chain standards of the International Standardization Organization (ISO), the standards of the International Hydrographic Organization (IHO) as well as the IMO Compendium on Facilitation and Electronic Business

3. To strive for the introduction of port community systems and secure data exchange platforms in the main ports of all member states represented in the IMO

4. To review existing IMO Guidance on Maritime Cyber Risk Management on its ability to address cyber risks in ports, developing additional guidance where needed

NOTE

1. Read the full call to action posted June 2, 2020, on the World Ports Sustainability Program website: https://sustainableworldports.org/port-and-shipping-industry-partners-in-urgent-call-to-action-to-accelerate-pace-of-digitalization/.

5. To raise awareness, avoid misconceptions, and promote best practices and standardization on how port communities can apply emerging technologies such as artificial intelligence (AI), advanced analytics, internet of things (IoT), digital twins, robotics process automation, autonomous systems, blockchain, virtual reality (VR), and augmented reality (AR)

6. To facilitate the implementation of such emerging technologies and other innovative tools to increase health security in port environments, allowing port and marine employees, contractors, and the vessel crew to work and interact in the safest possible circumstances

7. To develop a framework and roadmap to facilitate the implementation and operation of digital port platforms where authorized port community service providers and users can share data under secure data sharing protocols, enabling these platforms to connect with hinterland supply chains as well

8. To establish a coalition of willing stakeholders to improve transparency of the supply chain through collaboration and standardization, starting with the long-overdue introduction of the electronic bill of lading

9. To set up a capacity-building framework to support smaller, less developed, and under- staffed port communities, not only with technical facilities, but also with personnel training. Quality data exchange requires a trained workforce with mid- and long-term perspectives to build, implement, support, and sometimes override technology

22. ***The implementation of these priorities will require collaboration between maritime supply chain industry stakeholders, governments, and multilateral and bilateral development partners.*** Above all, successful implementation calls for intergovernmental collaboration; the acceleration of digitalization will require change management at local, regional, and national levels, fostering the need to implement an institutional framework. The IMO secretary general supported this call to action and encourages collaboration between maritime supply chain industry stakeholders and member states as well as intergovernmental collaboration in addressing the nine priorities for accelerating digitalization highlighted in the statement.

Above all, successful implementation calls for intergovernmental collaboration; the acceleration of digitalization will require change management at local, regional, and national levels, fostering the need to implement an institutional framework.

23. ***However, the move to fully digitize port authorities and ports communities also raises new risks in terms of cybersecurity.*** In 2017, global container shipping company Maersk and its international port operation wing overcame an aggressive cyberattack—which served as a serious wake-up call. More recently in 2020, MSC, a global container shipping company, had its digital tools and website (www.msc.com) hacked over the long Easter holiday weekend. Since the attack on MSC, several other large shipping companies have discovered cyberattacks dating back over the past three years—and most certainly, more attacks will come. In 2019, ENISA, the European Union Agency for Cybersecurity, warned that cyberattacks on PCSs could lead to the physical shutdown of operations in an affected port, with all the concomitant impacts on food security, business continuity, and cost. Thus, improving cybersecurity stands as a key parallel priority for public and private stakeholders in maritime trade and logistics. As discussed further in chapter 5 of this report, the time has come to not only initiate, but more crucially, to expand the cybersecurity dialogue within and between port communities in order to develop collaborative approaches and enhance cooperation between public and private sector stakeholders.

24. ***Finally, this report underlines digitalization as not solely a technological issue, but also as human capital and institutional issues.*** Any move towards increased digitization will require a high level of political commitment, while the establishment must have an appropriate legal, regulatory, and policy framework at the national level, across the different disciplines of the maritime, port, clearance agencies, and the transport and logistics sector. This move toward digitalization will also require improvements in human capital to commission, absorb, and implement the associated demands on stakeholders. Overcoming this challenge will necessitate considerable efforts; therefore, this report proposes establishing a national-level framework to manage the change. Discussed in chapter 6, the framework encompasses three levels: an interministerial committee, a steering committee, and a business process committee.

Chapter 2:
The Digitization Agenda

2.1 The Need for Digitization

25. ***Maritime transport remains the backbone of globalized trade and the manufacturing supply chain, with more than four-fifths of global merchandise trade (by volume) carried by sea.*** The maritime sector offers the most economical and reliable mode of transportation over long distances. Volumes carried have increased at an annual average of 3 percent over the period from 1970 to 2018. The total volumes carried at sea reached a milestone of 11 billion metric tons in 2017, driven by growth in dry bulk commodities, followed by containerized cargo, other dry bulk, oil, gas, and chemicals (UNCTAD 2019). While the growth in maritime volumes fell slightly in 2018, the pre-COVID-19 projections had estimated continued growth of 2.6 percent in 2019, and then a return to a compound annual growth rate of 3.4 percent over the period from 2019 to 2024.[1]

26. ***The impact of the COVID-19 pandemic has been profound, bringing economic activity to a near standstill, disrupting lives, and engendering significant social and economic costs.*** The economic damage is already evident and represents the largest economic shock the world has experienced in decades. The Global Economic Prospects Report (World Bank 2020) baseline forecast envisions a 5.2 percent contraction in global gross domestic product (GDP) in 2020, the deepest global recession in decades, despite the extraordinary efforts of governments to counter the downturn with fiscal and monetary policy support. Across the longer horizon, the deep recessions triggered by the pandemic are expected to leave lasting scars through lower investment, an erosion of human capital through lost work and schooling, and fragmentation of global trade and supply linkages.

27. ***One of the early lessons to emerge from the pandemic has been the critical role the maritime ports and their associated infrastructure play in the supply chain.*** Ships can carry large volumes of merchandise, provided that producers and consumers have access to adequate and effective infrastructure at the seaports and along the inland logistics chain to transport the volumes, in whatever form. The shortages of some basic supplies in developed countries during the early days of the pandemic revealed the fragility of the current logistical system in all countries, along with the need to both ensure business continuity and improve resilience of those infrastructures going forward.

NOTE

1. Based on an income elasticity and the IMF GDP forecast pertaining at the time (see UNCTAD 2019).

The maritime sector offers the most economical and reliable mode of transportation over long distances.

28. ***More generally, how ports perform represents a crucial element in the cost of trade for any country.*** Poorly performing ports reduce trade volumes, an impact particularly pronounced for landlocked developing countries and the small island developing states. The port, together with the hinterland access infrastructures (whether inland waterway, rail, or road) constitutes a crucial link to the global marketplace and needs to operate efficiently. Efficient performance encompasses a myriad of factors, including the efficiency of the port itself, the availability of sufficient draught and dock facilities, the quality of the connections to road and rail services, the competitiveness of those services, and the efficacy of the public agencies involved in clearance. Inefficiencies or nontariff barrier in any of these actors will result in higher costs, reduced competitiveness, and lower trade (Kathuria 2018).

The total volumes carried at sea reached a milestone of 11 billion metric tons in 2017

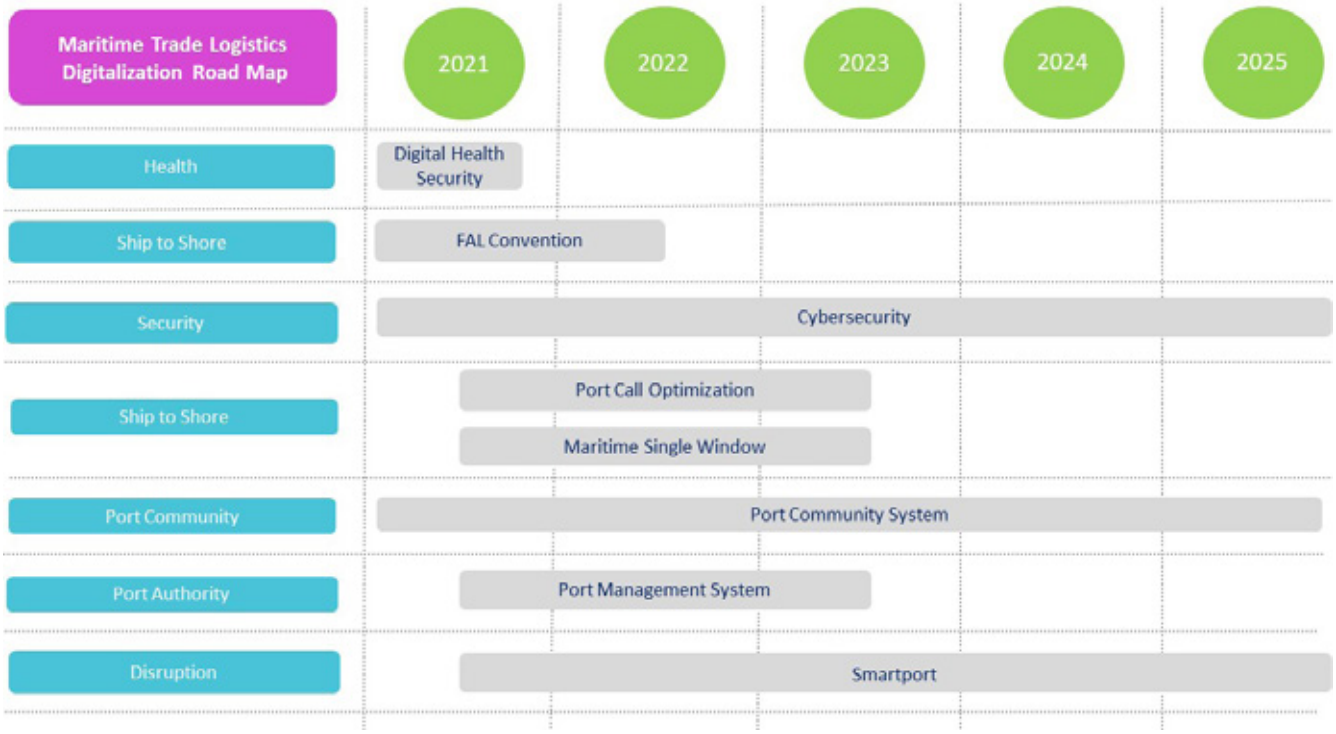
29. ***Port performance is not only dependent on the scale of the physical infrastructure; the institutional infrastructure is almost as, if not more, important.*** The efficient functioning of a port, and its access infrastructure, needs four types of assets overseeing the importance of an appropriate regulatory and policy framework: First, the physical infrastructure, for example, sufficient draught for the vessels to access and egress the port, sufficient quay space and superstructure (cranes, for example) to load and unload the vessels, and the ability to efficiently move consignments in and out of the port to the origin or destination. Second, the digital infrastructure—which ensures the efficient use of the physical infrastructure and is the subject of this report. Third, the institutional, or soft, infrastructure, which includes all the administrative and clearance services (customs, phytosanitary, and others) necessary to facilitate the import, export, and transit of goods, plus the supportive information and communications technology (ICT). Finally, the human capital in the port administration, operations, and marine services as well as the logistics sector supporting the port. While the overall efficiency of any port depends on an appropriate quality of all four assets, this report focuses on the latter two aspects, specifically the digitization agenda and the concomitant need to protect and develop human capital in the sector.

30. ***The available comparable indices indicate the impact of inefficiency on international trade.*** The World Bank Logistics Performance Index (LPI) and Doing Business Index (DBI) on trading across borders and the World Economic Forum's Global Competitiveness Index (GCI) 4.0, on efficiency of seaport services and border clearance, indicate the extent to which inefficiencies at a nation's sea borders can impact international trade competitiveness. Technological innovations and digitalization provide opportunities to foster a more holistic approach and integrate the port ecosystem facilitating trusted partner collaborations between government agencies and the private sector and to realize significant efficiencies in port transactions.

2.2 A Schematic Timeline

31. ***Figure 2.1 provides a schematic of the road map for a country, port, and port community to follow in digitizing the maritime logistic chain.*** The proposed road map advocates the need for a holistic approach. The figure illustrates the necessary short-, medium-, and longer-term measures to protect public health, ensure business continuity, and improve and protect the resilience of the system.

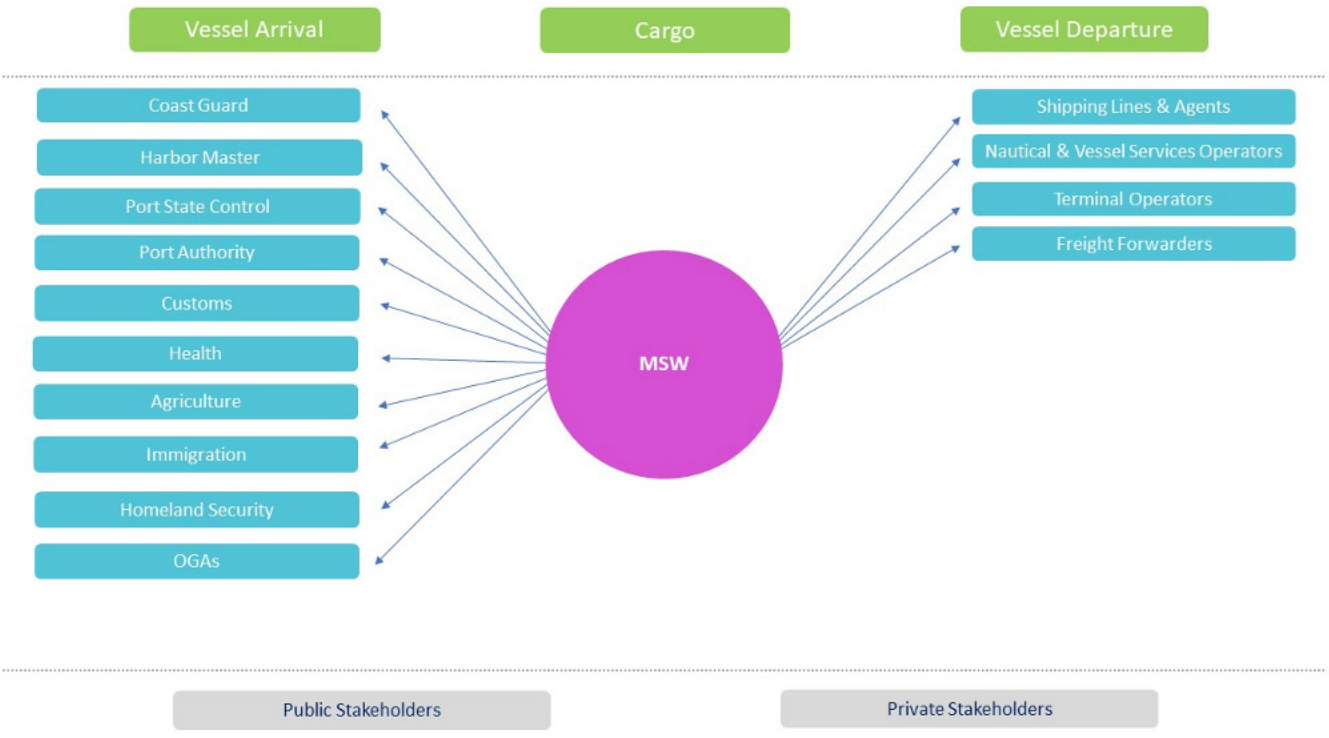
Figure 2.1. Maritime Trade Logistics: Digitalization Road Map



32. ***The first stage involves the crucial emergency measures in terms of digital health security monitoring and the establishment of crisis management centers within intergovernmental agencies.*** The overarching objective is to protect vessel crews, port workers, and passengers from cruises and ferries in the "new normal" by enforcing social distancing and the temperature control of port workers.

33. ***The second stage involves the introduction of the short-term measures to meet the mandatory requirements defined in the International Maritime Organization's Facilitation (FAL) Convention (IMO 1965).*** The FAL Convention aims to support transmission, receipt, and response of information required for making the transition to full-fledged maritime single windows, for example: the arrival, stay, and departure of ships, persons, and cargo via electronic data exchange (figure 2.2), thereby minimizing the number of paper-based and people-based contacts. This has been a mandatory requirement for all ports since April 2019, though implementation remains partial at best.

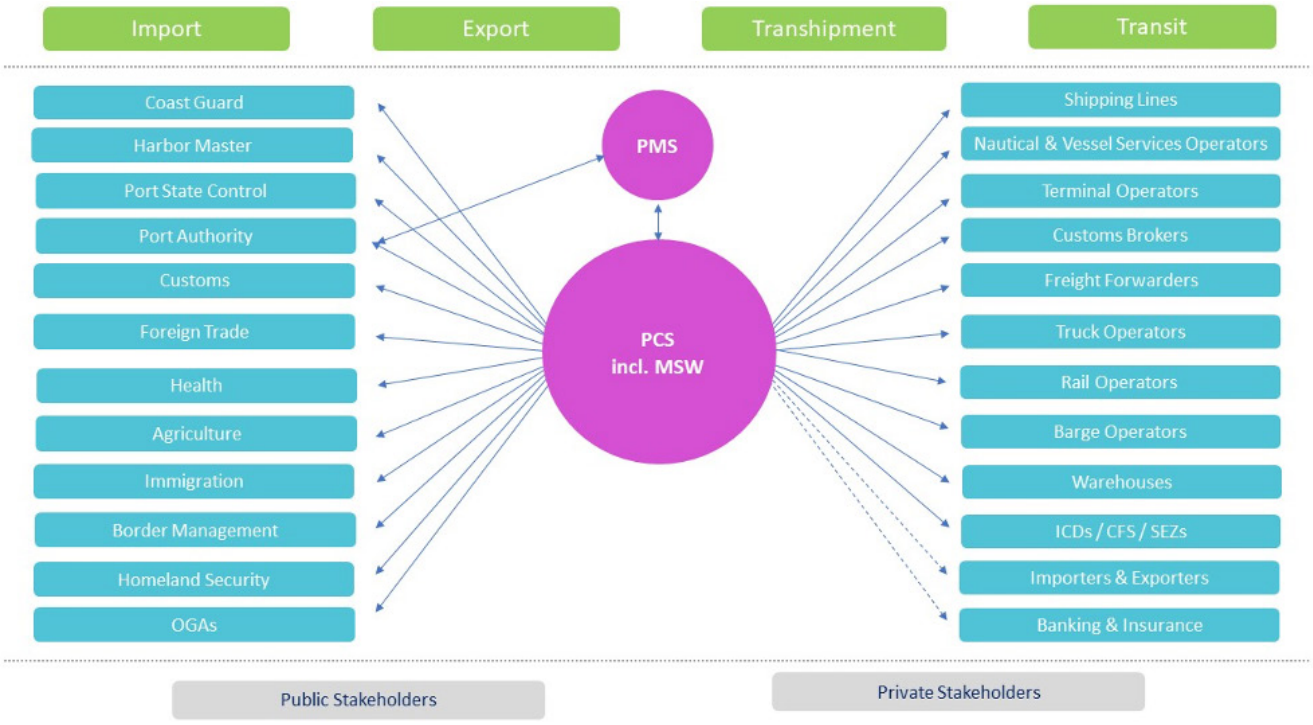
Figure 2.2. Maritime Single Window



34. ***In parallel to the need for ports to meet the mandatory requirements of the FAL Convention, discussions must be held on the nine key data elements related to port call optimization.*** Port call optimization allows ships to optimize their speed during the voyage to facilitate a timely arrival at the pilot boarding place, thus securing berths, fairways, and nautical services at the destination ports. This just-in-time (JIT) arrival will also increase a port's relative attractiveness and hence its competitiveness.

35. ***Ports must also commence the establishment and introduction of a port community system.*** A port community system, is a platform to optimize, manage, and automate the port and logistics processes through a single submission of data in the transport and logistics chain (see figure 2.3). The coherence between the port community system, port management system, and maritime single window should be ensured to allow the maritime and trade logistics actors to benefit from the digitalization of these processes and associated applications, logically culminating in the smart port.

Figure 2.3. Port Community System: Optimal Architecture



36. ***Importantly, increasing the digitization of the maritime logistical chain, while essential, also brings new risks.*** Between February and May 2020, cyberattacks increased 400 percent in the maritime industry (Captive International 2020). The risk of a cyberattack has emerged as the top risk for port authorities and the wider port community of stakeholders, necessitating improved cybersecurity at the port community ecosystem level. The next two chapters present in more detail the recommended measures, delineated between those measures recommended for immediate implementation and those recommended for short-term implementation, followed by those that are recommended for medium-term implementation.

REFERENCES

Captive International. 2020. "Maritime Businesses See Fourfold Increase in Cyber Attacks Since February: Astaara." June 23, 2020. https://www.captiveinternational.com/news/maritime-businesses-see-fourfold-increase-in-cyber-attacks-since-february-astaara-3568.

IMO (International Maritime Organization). 1965. Convention on Facilitation of International Maritime Traffic, as amended in 2016. https://www.imo.org/en/About/Conventions/Pages/Convention-on-Facilitation-of-International-Maritime-Traffic-%28FAL%29.aspx.

Kathuria, Sanjay. 2018. A Glass Half Full: The Promise of Regional Trade in South Asia. Washington D.C.: The World Bank Group. https://openknowledge.worldbank.org/handle/10986/30246.

UNCTAD (United Nations Conference on Trade and Development). 2019. Review of Maritime Transport. Geneva: UNCTAD. https://unctad.org/webflyer/review-maritime-transport-2019.

World Bank. 2020. Global Economic Prospects, June 2020. Washington D.C.: World Bank. https://openknowledge.worldbank.org/handle/10986/33748. License: CC BY 3.0 IGO.

Chapter 3: Immediate and Short-Term Recommendations

3.1 Introduction

37. ***Chapter 3 provides an overview of recommended immediate and short-term measures, in terms of digital health security for countries, port authorities, and ports to implement.*** Short term is defined here as, ideally, between three and twelve months; however, this is a recommended timeline to clearly underscore the urgency of the agenda, as an aspiration rather than a definitive timeline.

3.2 The Immediate Recommendations

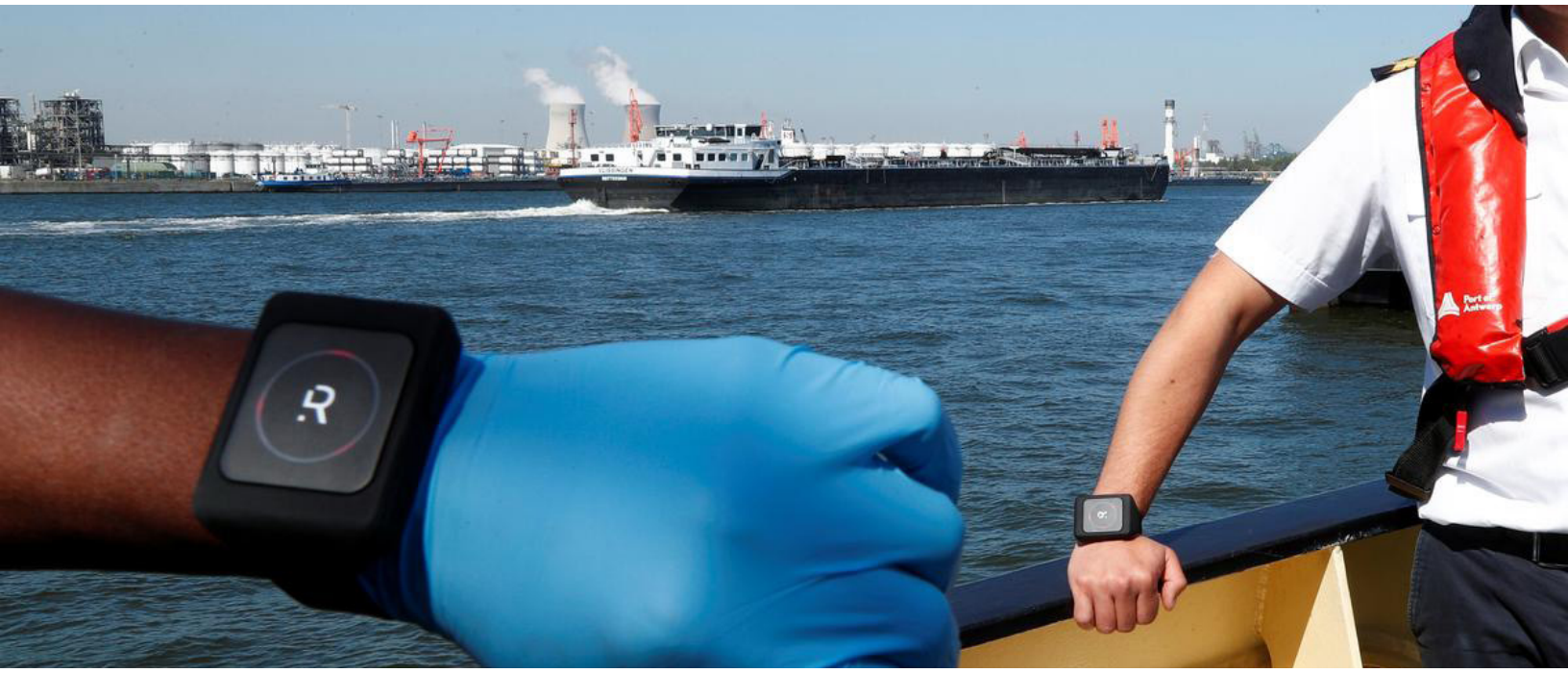
3.2.1 Improving Digital Health Security

38. ***The impact of the COVID-19 pandemic on global healthcare systems has underlined the need to improve digital health security at critical infrastructure, such as ports, to protect workers.*** Digital health security consists of those digital measures designed and implemented to protect the health and welfare of port workers, and involve such measures as the enforcement of social distancing rules and the temperature control of port workers through the use of technologies such as thermal cameras, drones, and electronic wearables, which could be integrated into a digital port security command and control center.

ELECTRONIC WEARABLES

39. *The COVID-19 pandemic continues to have a dramatic impact on the global logistics and supply chains and requires the identification of creative solutions to facilitate business continuity in the "new normal."* One of the most widely adopted, if not always obeyed, measures is the introduction of maintaining social distance. The introduction of maintaining a defined distance between individuals (the actual distance varies by country and sometimes by mode) has challenged normal business workflows and processes and inspired companies to find new solutions to guarantee worker safety and health.

40. ***The Port of Antwerp in Belgium is currently piloting one of the most interesting examples of digitized solutions.*** The Port of Antwerp has partnered with a Belgian startup, which specializes in future-proof internet of things (IoT) solutions for maritime services, port terminals, and petrochemical plants. The latter's mission is to support the global digitization of the port industry and help shape the port of the future. In 2019, the startup developed a wearable device, similar to the more industrial wearables in the market, but equipped with several security and safety applications, particular to the port context. At the end of February 2020, the startup added a new function to monitor and maintain the physical distancing required, and to facilitate contact tracing through device-to-device communication.



41. ***In order to assess the new functionality in a professional and complex environment, the Port of Antwerp collaborated with the startup to conduct several tests.*** In particular, the tests focused on man-to-machine detection, man-down detection, safe work in closed spaces, and a lone worker alarm (that includes a panic button and man-down detection). As the extent of the COVID-19 pandemic unfolded in the spring of 2020, radius testing of the wearable electronic device was performed at the end of April, which also garnered media attention (figures 3.1, panels a and b).

42. ***These tests were conducted during standard 12-hour shifts worked by the port authority's technical and nautical staff.*** In total, eight different individuals participated in the pilot: five boatmen tested the device outdoors, on a lock platform while assisting vessels to moor in the lock, and three vessel traffic operators tested the wearables in an indoors working environment. Privacy protection is included by design and the device is fully compliant with the data protection regulations; the devices store no personal data. The device itself generates a soft signal (vibration and orange indicator light) when the distance between two or more devices is closer than 2 meters. A second and more explicit signal (loud alarm, vibration, and red flashing indicator) is generated when a device detects less than 1.5 meters of distance between devices. This test included a technical evaluation as well as a user experience interview.

Figure 3.1. Port of Antwerp: Pilot Testing of Electronic Wearable Device

a. Radius testing of wearable device (April 2020)

b. Port of Antwerp discusses COVID-19 bracelet on CNBC

43. ***Both tests yielded positive results, with users considering the wearable helpful in ensuring workers maintain the 1.5-meter distance.*** Users also spoke of being surprised at the dimensions of this distance, indicating a tendency to misjudge what was required to maintain the separation. At a technical level, the device passed all tests and remained fully functional within a defined radius, despite the presence of several elements that could have blocked or jammed the signal. Further testing in more specific and difficult working conditions will be executed in the coming months, though the preliminary results indicate an electronic wearable will have a role in the post COVID-19 "normal" working environment.

THERMAL CAMERAS

44. ***Thermal cameras have helped with epidemic prevention and control in many settings and many countries.*** For example, thermal cameras were introduced at many points of entry during the 2014–16 Ebola outbreak in West Africa. In comparison to the traditional methods of measuring body temperature, thermal cameras offer a significant improvement in speed and accuracy. In the maritime sector, Port Coronel in Chile became one of the first ports to introduce this technology in the early days of the COVID-19 pandemic, placing the devices in the main access areas and in the logistics center of cargo terminals, to measure with a high degree of precision the body temperature of workers entering the terminal. Cameras are also used to monitor the temperature of the passengers at ferry and cruise terminals, with Portsmouth International Port being the first port in the United Kingdom to install such a scanner to help ensure passenger safety.

45. ***However, thermal cameras should not be considered a panacea.*** While thermal imaging systems generally detect a high body temperature accurately when used appropriately, they do not detect any other infection symptoms, and a high body temperature does not necessarily mean a person has a COVID-19 infection—thus highlighting the need for additional testing to confirm the initial abnormal finding. In addition, one of the major disadvantages associated with the use of a thermal camera, or even the more orthodox measures of body temperature, is the relatively high proportion of individuals infected with COVID-19 who are contagious, test positive, but remain asymptomatic. Recent research suggests this number could be as high as 40 percent.1

NOTE

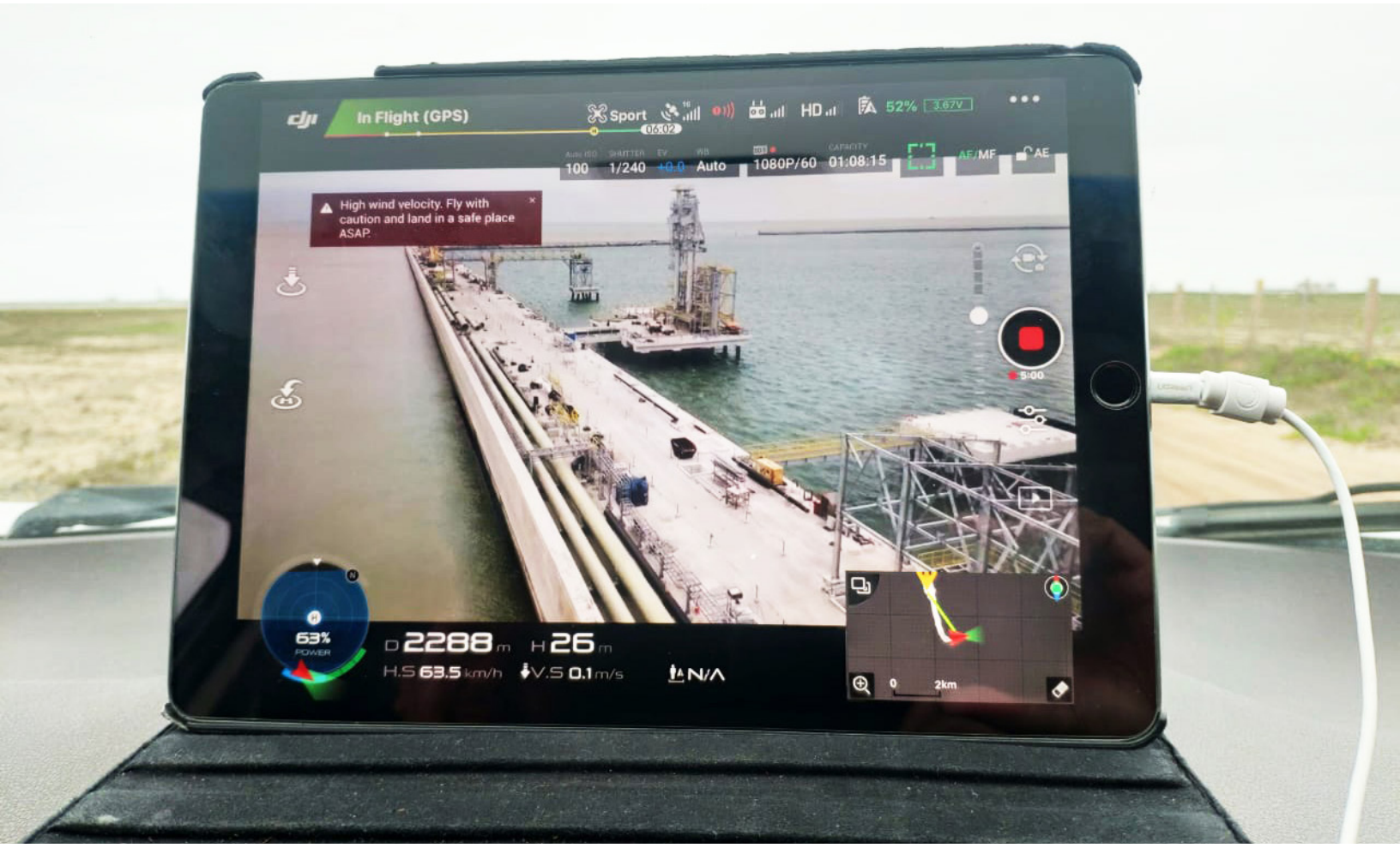
1. The latest guidance from the United States Center for Disease Control estimates that 40 percent of infected individuals may be asymptomatic. See https://www.cdc.gov/coronavirus/2019-ncov/hcp/planning-scenarios.html.

UNMANNED AIRCRAFT SYSTEMS: DRONES

46. ***The formal definition of an Unmanned aircraft system (UAS) is any aircraft intended to be flown without a pilot on board.***[2] Now available in a variety of types, UAS are designed with different capabilities to fit user needs, such as autonomous (no pilot input) or remotely piloted modes of operation. The more common term adopted by the media and understood by the public is "drone." UAS provide a prime example of an emerging technology in the new industrial era. Characterized by significantly lower costs and complexity when compared with manned systems, these flying robots have the potential to unlock the lower skies as a mobility resource and enable new applications, and are being increasingly used to improve efficiency and reduce cost of delivering medical supplies and blood (as done in Rwanda and Ghana). In addition, demand is accelerating for more established uses such as survey and mapping applications, land digitization and tenure, agriculture and precision farming, infrastructure and construction monitoring as well as disaster risk management.

NOTE

2. The definition of unmanned aircraft systems (UAS) was presented at the International Civil Aviation Organization's (IACO) First Meeting of the Asia/Pacific Unmanned Aircraft Systems Task Force (APUASTF/1) in Bangkok, Thailand, held April 3–5, 2017. For more details see the meeting agenda document, "Terminology and Concepts Describing Unmanned Aircraft Systems," available online: https://www.icao.int/APAC/Meetings/2017%20APUASTF1/WP07.pdf.



47. ***The not yet fully realized, ports have recognized the potential uses of UASs for enhancing operations.*** Pilots have already been undertaken in a number of ports, including, among others, Antwerp, Rotterdam, and a number of ports in the United Kingdom, testing drone use in areas such as asset management, environmental sustainability, and security (Green Port 2019). As one example of an emerging use, the Norwegian Maritime Authority (NMA) conducted sulfur emissions testing using a drone in 2019, and has announced plans to purchase three new sulfur sensors as part of its cooperation with the coast guard and the Norwegian Radiation Protection Authority to monitor and ensure vessel emissions meet the new maximum limit (0.5 percent of sulfur in marine fuels) now mandated by the IMO and the European Union (European Commission 2020). In the context of the COVID-19 pandemic and the maritime sector, drones have been used at ports to enforce social distancing and face-mask wearing, monitor crowds, facilitate aerial broadcasting, spray disinfectant, conduct aerial thermal sensing, monitor traffic, and deliver medical supplies at ships.

48. ***An example from Belgium illustrates how drones could be implemented to increase public safety.*** Within three weeks after the COVID-19 lockdown in mid-March 2020, the Port of Antwerp was ready to implement an automated drone solution to monitor social distancing at the largest truck parking in the port (which holds approximately 200 trucks), as most drivers come from countries other than Belgium and find it challenging to understand the country's regulations on social distancing. Unfortunately, the automated drone could not be operated due to pending official approval by the responsible authority. Instead, large digital screens were used to inform the drivers, with notifications in eight languages. Similarly, in the United States, port police at the Port of Los Angeles in California are using drones to enhance public safety across port operations (Link-Wills 2020).

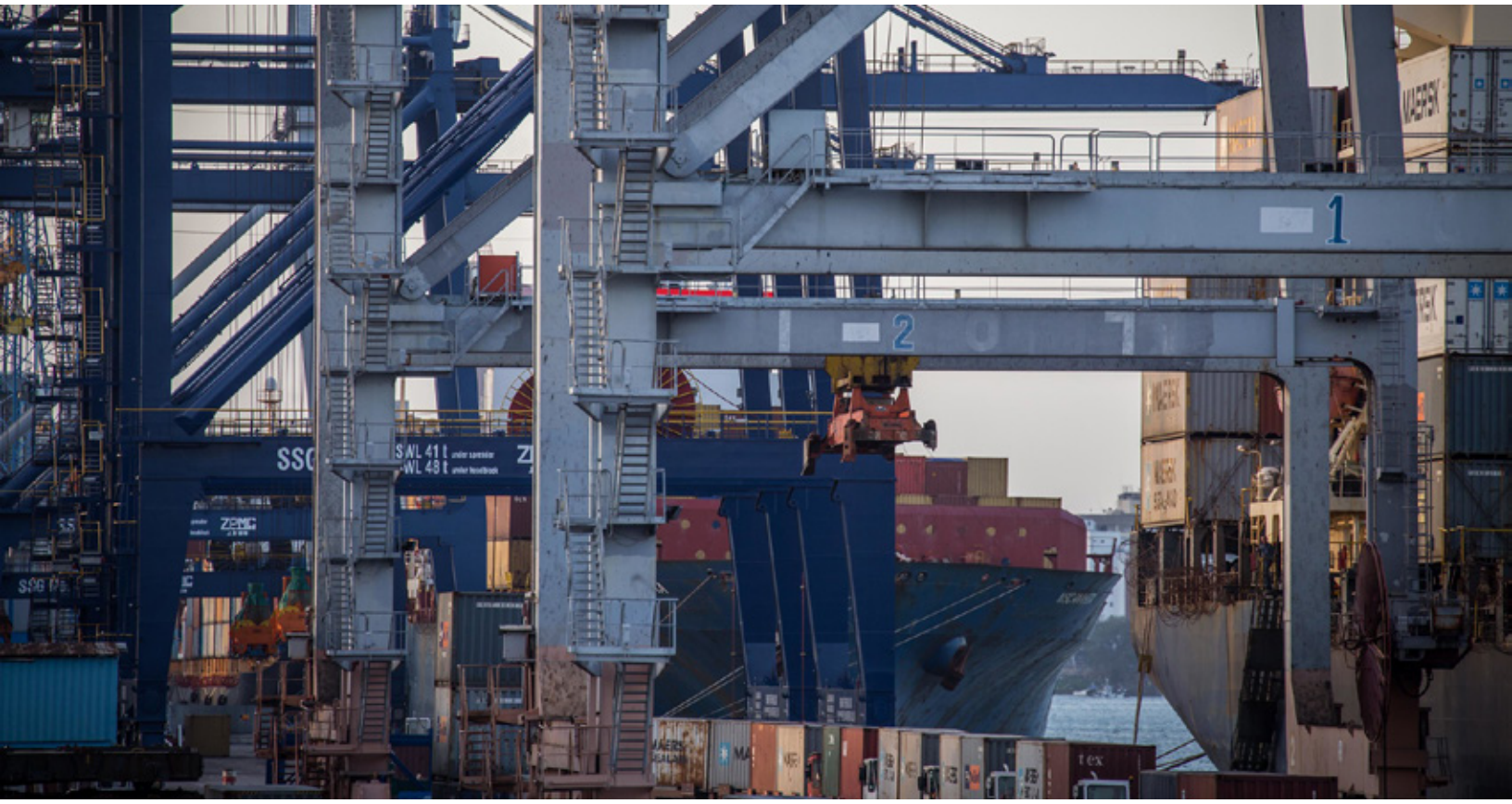
In the context of the COVID-19 pandemic and the maritime sector, drones have been used at ports to enforce social distancing and face-mask wearing, monitor crowds, facilitate aerial broadcasting, spray disinfectant, conduct aerial thermal sensing, monitor traffic, and deliver medical supplies at ships

3.2.2 Establishing a Crisis Management Platform

49. ***Early lessons learned from the pandemic include the need to ensure coordination across all the relevant public agencies.*** During COVID-19, cross-agency cooperation is critical to ensuring business continuity in the maritime sector. This coordination helps establish a digital crisis management platform that integrates all government agencies related to maritime trade, manage crew health and crew changes, ensure sufficient stocks of critical equipment—such as masks, tests and drugs—monitor hospitals and immigration needs in real time, anticipate the evolution of the crisis, and propose measures to control the pandemic at the port community level. More than nine months into the pandemic, coordination of this type remains an immediate priority. Two recent developments in this sphere include the Philippines Port Authority September 2020 rollout of a COVID-19 electronic tracing system specifically designed for the port context (PPA 2020), and the development, by technology companies such as Thales Group, of commercial electronic crisis management platforms that integrate "the power of big data, artificial intelligence, and cybersecurity."[3]

NOTE

3. See the Thales Group webpage, "Solutions for the Covid-19 Crisis in the Field of Public Safety." Accessed November 2020: https://www.thalesgroup.com/en/solutions-covid-19-crisis-field-public-safety.



3.3 The Short-Term Recommendations

50. ***After the immediate digital measures above, the following measures are recommended to follow as closely as feasible, and ideally within a period of 12 months.*** These measures are intended less to ensure immediate business continuity, as in the previous cases, than to meet the mandatory requirements, improve resilience and efficiency, and protect business continuity in future. Hence, this section will discuss short-term measures for the port community ecosystem, including the introduction of electronic data interchange (EDI) and the maritime single window (MSW), under the Convention on the Facilitation of International Maritime Traffic (the FAL Convention), port call optimization, and the establishment of port community systems (PCSs) for port authorities to communicate with all port stakeholders to improve the resilience of the maritime logistic chain.

3.3.1 Electronic Data Interchange and the FAL Convention

51. ***Ships, crew, goods, and passengers that travel across national borders are subject to a range of government controls, both on arrival and departure.*** These controls address a wide range of issues, including public health, revenue protection, security, immigration, controls on import and export, and sanctions enforcement. A range of practical procedures and processes must be followed to ensure maritime safety as well as the provision of general port services to ships. As with the regulatory controls, these could be due to national or regional requirements or mandated by international conventions and agreements. All of these controls and procedures, whether local, national, international, regulatory, or commercial, have features in common—all require the provision of information to a range of different agencies and entities, and require action taken by ships, crews, and ports. The process by which this myriad of regulations, requirements, and procedures are simplified and harmonized is known as "facilitation" and forms an integral part of the World Trade Organization Agreement on Trade Facilitation (WTO TFA Agreement), adopted in 2018.

A range of practical procedures and processes must be followed to ensure maritime safety as well as the provision of general port services to ships.

WHAT IS A FAL CONVENTION ELECTRONIC DATA EXCHANGE?

52. ***The need for standardization and reduction of unnecessary bureaucracy in the maritime sector was recognized by the International Maritime Organization (IMO).*** In response, the IMO was developed the FAL Convention,[4] which has been in force since 1967 and ratified by 124 member countries. The FAL Convention is updated on a regular basis by member governments through the FAL Committee—which meets once a year at the IMO headquarters in London. The convention's main objectives are to prevent unnecessary delays in maritime traffic, to aid cooperation between governments, and to secure the highest practical degree of uniformity in formalities and other procedures. The convention contains standards and recommended practices for ports to simplify formalities, documentary requirements, and procedures on the arrival, stay, and departure of vessels. It also encourages the use of standardized FAL forms by authorities and governments in requesting necessary information from the master or ship's agent in relation to controls and procedures. The necessary information, and the relevant forms covering all data requested by public authorities' regulatory requirements under the FAL Convention include the following:[5]

- IMO General Declaration (FAL form 1)
- Cargo Declaration (FAL form 2)
- Ship's Stores Declaration (FAL form 3)
- Crew's Effects Declaration (FAL form 4)
- Crew List (FAL form 5)
- Passenger List (FAL form 6)
- Dangerous Goods Manifest (FAL form 7)
- Security-related information as required under International Convention for the Safety of Life at Sea (SOLAS) (regulation XI-2/9.2.2)
- Advance electronic cargo information for customs risk assessment purposes
- Advanced notification form for waste delivery to port reception facilities

53. ***In any port call, the submission of this information involves a wide range of stakeholders.*** Shipping companies engaged in international trade must submit large volumes of information and documents to terminal operators, port authorities, and other public sector bodies, in order to comply with regulatory and port entry requirements. These include, inter alia (Latin for "among other things"), maritime agencies, customs, health, border police, immigration,

NOTES

4. The IMO's Explanatory Manual to the Convention on Facilitation of International Maritime Traffic (FAL.3/Circ.215), reviewed and updated by FAL 42 on April 12, 2019, contains guidance and interpretation of the provisions of the annex of the FAL Convention. https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/FAL%20related%20non-mandatory%20documents/FAL.3-CIRC.215.pdf.

5. See the full list of FAL Convention documents, available as PDFs, on the IMO website: https://www.imo.org/en/OurWork/Facilitation/Pages/FormsCartificates-default.aspx.

agriculture, and defense authorities. Often information must be submitted through several different authorities, each with its own specific system and/or paper forms. These requirements, together with the associated compliance costs, constitute a burden both to governments and to the business community. The inefficiencies and resulting increase in costs represent a major barrier to the development of international trade, particularly in the less developed countries.

WHAT IS A FAL CONVENTION ELECTRONIC DATA INTERCHANGE?

54. ***Accordingly, the FAL Convention makes a number of recommendations for member governments to improve coordination and communication between parties.*** The first stage is the introduction of electronic data interchanges between ship and ports, commonly known as EDI. An EDI system is intended to simplify the process of providing and sharing the necessary information to fulfill regulatory requirements for both authorities and shipping industry, and removes the need for successive paper submissions and the associated time requirements. Its use can result in improved efficiency and effectiveness of official controls, while also reducing costs for both business and administrative parties. The FAL Convention obligates public authorities to establish systems for the electronic exchange of information, with an original deadline of April 8, 2019—subsequently extended to April 8, 2020.

The FAL Convention obligates public authorities to establish systems for the electronic exchange of information

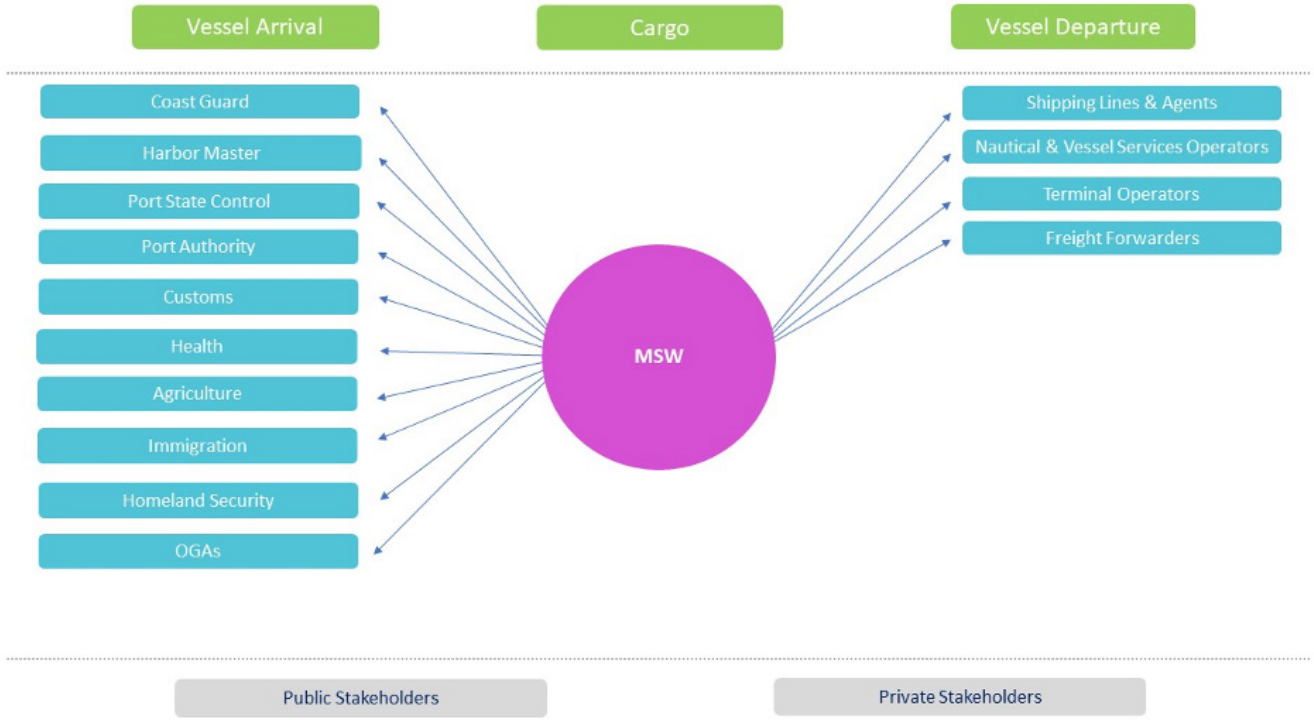
55. ***In addition, the FAL Convention encourages the use of the maritime single window concept, to enable all information required by public authorities in connection with the arrival, stay, and departure of ships, persons, and cargo, to be submitted via a single portal without duplication.*** Establishing a single window, facility delivers several benefits: enhances the availability and handling of information, simplifies and expedites information flows between trade and government, and brings about greater harmonization and better sharing of the relevant data across governmental systems, resulting in meaningful gains to all parties involved in cross-border trade. Public authorities may require the same identical data for different purposes, including identification of the ship, date and time of arrival, port of departure, and cargo information; however, combining, harmonizing, and minimizing the information required from ship masters and agents has been a longstanding request from trade, an issue which could be addressed through the MSW concept.

56. ***The FAL Convention defines "single window" as a facility that allows submission of standardized information covered by the FAL Convention to a single-entry point.*** Clearance processes can be facilitated by combining common and harmonized data elements into a single message according to commonly agreed standards and format and sent electronically to a single official destination, rather than being sent to each authority separately. The FAL Committee issued revised guidelines for setting up an MSW[6] to serve as a source of information, advice, and guidance for interested member states. The guidelines also provide examples of the experience and knowledge gained by some member states in approaching implementation (figure 3.2).

NOTE

6. See Guidelines for Setting Up a Maritime Single Window (FAL.5-Circ.42) dated May 16, 2019. https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/FAL%20related%20nonmandatory%20documents/FAL.5-Circ.42.pdf.

Figure 3.2. Maritime Single Window



57. ***However, despite the advantages, the number of countries that have developed a fully functional MSW remains low.*** To date, many countries have developed parallel single windows addressing the needs of different authorities, requiring traders to submit the same information more than once to several single windows. Thus, realizing the full benefits of the MSW concept will involve a consolidated move toward a definitive single window covering all aspects of regulations and business to government exchanges of data. Box 3.1 provides an example of the benefits of a fully functional MSW.

Box 3.1

Box 3.1. Benefits of a Functional Maritime Single Window: VUMPA and the Case of Panama

In 2017, the Panama Maritime Authority and the Panama Canal Authority announced the launch of an initiative to develop the Panama Maritime Single Window System (VUMPA), with the objective to facilitate international maritime transport—through simplification and harmonization of the processes—in compliance with the FAL Convention.

As part of the initiative, every ship must now declare the required information electronically through the VUMPA system, so that all government institutions carry out the risk assessment, prior to the arrival of the vessel, and that the first inspection of an international ship upon arrival is carried out by a single inspector of the Republic of Panama.

The Panama Canal and the Panama Maritime Authority estimate that the introduction of VUMPA has reduced the need for more than 300,000 paper forms and documents, improving the efficiency and carbon footprint of transhipment procedures and saving up to 3,260 person hours annually.

Source: Panama Canal website (https://www.pancanal.com/eng/).

58. ***The need for harmonized maritime-related data and common agreed standards led to the development of the IMO Compendium on Facilitation and Electronic Business.***[7] The IMO Compendium is a tool for software developers who design the systems needed to support transmission, receipt, and response via electronic exchange, of information required for arrival, stay, and departure of ship, persons, and cargo to or from a port. The compendium consists of an IMO data set and IMO reference data model[8] agreed by the main organizations involved in the development of standards for the electronic exchange of maritime-related information linked to the FAL Convention. These organizations include the World Customs Organization (WCO), the United Nations Economic Commission for Europe (UNECE), and the International Organization for Standardization Technical Committee 8 (ISO/TC8, Ships and Marine Technology). The IMO, WCO, UNECE and ISO also collaborate under a new partnership to support increased maritime digitalization.

59. ***By harmonizing the data elements required during a port call and by standardizing electronic messages, the IMO Compendium facilitates the exchange of ship-to-port information and the interoperability of single windows, thereby reducing the administrative burden for ships linked to formalities and ports.*** The IMO Compendium is not conceived to create "new" standards, but rather as a tool to harmonize existing standards and produce guidance for interested

NOTES

7. The current IMO Compendium on Facilitation and Electronic Business is available online in an HTML version: https://svn.gefeg.com/svn/IMO-Compendium/Current/index.htm.

8. The IMO data set identifies and defines all the data elements related to reporting information requirements and the IMO reference data model establishes the underlying hierarchical data structure used in electronic data exchange.

parties to automatically map the IMO data set to any of the leading standards. The compendium also allows companies involved in maritime trade or transport to create software that can communicate across standards. This means that any organization responsible for a standard or a data model in the scope of a ship approaching a port is welcome to add and map data to the IMO Compendium.

60. ***Since July 2019, the Expert Group on Data Harmonization (EGDH) has been responsible for the technical maintenance of the IMO Compendium and for further expanding its data set and data model to areas beyond the FAL Convention.*** These include the exchange of logistics and operational port and shipping data and maritime services as provided in Resolution MSC.467(101) and MSC.1/Circ.1610 (documents available online at https://www.imo.org). The EGDH also aims to contribute to support electronic data exchange for all IMO instruments. The EGDH meets twice a year at IMO's London headquarters and brings together IMO member states, industry representatives, and key standards organizations involved in electronic exchange of information related to regulatory port clearance, including WCO, UNECE, ISO, IHO, and the International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA).

61. ***In light of the increase in the use of digitalized systems across the maritime sector, the FAL Committee has also considered the cyber risks.*** The objective is to protect the maritime transport network from cyberthreats, including the need to address particular risks to MSWs, processes for electronic certificates and data exchange between ships and shore, pre-arrival information based on the FAL Convention, and processes involving the ship–port interface. Relevant IMO guidance includes the Guidelines on Maritime Cyber Risk Management[9] to address cyber risks in the maritime domain and Resolution MSC.428(98), Maritime Cyber Risk Management in Safety Management Systems,[10] encouraging shipping companies to address cyber risks in their safety management systems. In an effort to establish guidelines on cybersecurity on ships, leading industry stakeholders have provided an overarching scope of nature in relation to cybersecurity, which chapter 5 will discuss in more detail.

NOTES

9. See the Maritime Safety Committee's Guidelines on Maritime Cyber Risk Management (MSC-FAL.1-Circ.3), dated July 5, 2017, and available online: https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/FAL%20related%20nonmandatory%20documents/MSC-FAL.1-Circ.3.pdf.

10. See the Maritime Safety Committee's Maritime Cyber Risk Management in Safety Management Systems (MSC.428-98), adopted June 16, 2017: https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/FAL%20related%20nonmandatory%20documents/RESOLUTION%20MSC.428-98.pdf.

3.3.2 Port Call Optimization

62. ***The arrival of a ship at the pilot boarding place at the precise time the berth, fairway, and marine services are waiting is called port call optimization.*** The Global Industry Alliance to Support Low Carbon Shipping (GIA) was officially launched on June 29, 2017, alongside the first Intersessional Working Group on the Reduction of Greenhouse Gas Emissions (ISWG-GHG) meeting at IMO headquarters. The aim of the GIA is to develop innovative solutions to address common barriers to decarbonizing the shipping sector.[11] The work of the GIA on the just-in-time (JIT) arrival of ship is a concept in which a ship maintains the optimal operating speed to arrive at the pilot boarding place to ensure availability of berth, fairway, and nautical services (such as pilots, tugs, and linesmen).

NOTE

11. The Global Industry Alliance (GIA) was established under the framework of the GEF-UNDP-IMO GloMEEP Project. A full update of the work of the GIA is set out in document MEPC 75/12/4 (Secretariat). For more information, see the GIA website: https://glomeep.imo.org/.

63. ***The JIT arrival concept has been identified by the GIA as a feasible opportunity to both reduce greenhouse gas (GHG) emissions[12] and improve port competitiveness.*** JIT also provides an opportunity for optimal utilization of port assets, improve safety and environmental outcomes, along with lower costs for shipping lines, shippers, terminals, and ports. Work on port call optimization (PCO) is led by the International Taskforce on Port Call Optimization, which has also

NOTE

12. Further information on the GIA's work on just-in-time arrival is set out in document MEPC 74/INF.34.

written the Port Information Manual, aimed at providing a better understanding of the data exchanged in the ship–port interface and of the existing international standards connecting ships and ports. The scope of data covers the data set of the ship–port interface data, directly or indirectly related to the port authority, based on a trade and port agnostic business process and taking into account compliance with IMO regulations, contractual obligations, and other relevant public authorities such as customs.

WHAT IS INVOLVED IN PORT CALL OPTIMIZATION?

64. ***The goal of PCO is to optimize sustainable supply chains, safe and sustainable berth-to-berth navigation, deadweight, port stay, berth utilization, and other port resources and services.*** Successful PCO results in greater safety, a cleaner environment, and lower costs for shipping lines, shippers, terminals, and ports. In order to improve the quality and availability of data in the ship–port interface, the following data points are fundamental for optimizing: (a) the movement of the vessel—"Where is the berth? When is it available? and (b) the cargo on board—Where is the cargo? When is it available for hinterland transport?

The quality and availability of data plays an integral role in the journey toward port call optimization; data standardization represents the first vital step in the process.

65. ***The quality and availability of data plays an integral role in the journey toward port call optimization; data standardization represents the first vital step in the process.*** The following paragraphs look at how a port should handle data to achieve PCO.

- Data sharing by the data owner is an important aspect of improving data quality and availability. If data are not shared by the data owner, data updates might be delayed, and the data are not binding. However, data owners currently struggle to share data, as much data are in different standards and formats and at different times. However, data owners prefer to share one file to many users, to minimize the administrative burden and avoid errors and delays in update. Efficient, accurate data sharing requires standardization, which again requires investments in databases and in a culture change of people. For this reason, scoping the data is a critical two-part step: first to select the data elements needed to achieve compliance with IMO regulations and other standards, and then to select the data elements with the most impact to justify investments.

Data sharing by the data owner is an important aspect of improving data quality and availability.

- To ensure these investments in databases or culture change remain sustainable for ports and shipping alike, the most robust standardization body for both shipping and ports should be selected for each data element; in this way, standards will be maintained and available for the foreseeable future. Acceleration and acceptance of digitalization in the ship–port interface depend on both shipping and ports committing to the same standardization bodies—to avoid a proliferation of solutions and incompatibility between standards and systems, and, ultimately, futile investments into implementing standards that are either not fit for purpose or not viable for all stakeholders across the supply chain.

- Finally, planning such investments requires a road map per data set to understand when a particular standard becomes available for implementation, as realizing full interoperability of data requires not only the data element definition, but also a logical data model, application programming interface (API) specification, and technical and business performance requirements. The timing of each step is important in planning investments in standardization between shipping and ports.

- Shipping and port subject matter experts collaborate to select the most critical data elements in the ship–port interface necessary for compliance and with the largest impact on safety, environment, and security.

66. ***The priority list of nautical data elements includes data elements for (a) generic port data, (b) depth identification, and (c) location of terminals, berths, and berth positions.***

- With their strong impact on navigational safety and environment, these data elements are necessary to be compliant with the IMO's Code of Practice for the Safe Loading and Unloading of Bulk Carriers (known as the BLU Code)[13] and IMO Resolution A.893(21),[14] which regulates safe berth to berth navigation, and to be compliant with safe port clauses in Baltic and International Maritime Council (BIMCO) contracts. The latter is especially important in the tanker and dry bulk trade (representing about 85 percent of cargo ton miles in shipping), where charterers need to select the right ship to fit both the berth in the load port and the discharge port.

- With 93 member states, the most robust standardization body for these data elements is the International Hydrographic Organization (IHO), which has been working with national hydrographic offices since standards were first introduced.

- A submission to the IHO is made to define these data elements and realize real-time data exchange between a port authority and the national hydrographic office, which in turn delivers up-to-date electronic charts and books to ships to aid safe navigation. Hydrographic offices have a legal and moral obligation to provide accurate, contemporary data. The clear capture and sharing of data allow the adoption of best practices and helps to demonstrate the observance to due diligence. It ensures hydrographic offices and port authorities have worked together to discharge their collective SOLAS responsibilities for the benefit of each nation and the safety of the mariners. Accurate data sharing also strengthens the legal position of the port in the event of an incident. This submission has resulted in a working group with the highest priority within the IHO.

67. ***The priority list of administrative data includes three data elements necessary to complete notifications and declarations for in-port authorities such as customs and immigration, as follows: (a) update information in the IMO Global Integrated Shipping Information System (GISIS) database (***https://www.gisis.imo.org***), (b) accept ship data with IMO FAL Compendium data format and structure, and (c) plan for clearance.***

NOTES

13. Learn more about the IMO BLU Code and BLU Manual online: https://www.imo.org/en/OurWork/Safety/Pages/BLU-Code-and-BLU-Manual.aspx. Hard or digital copies can be purchased through an authorized IMO publications distributor: https://www.imo.org/en/publications/Pages/Distributors-default.aspx.

14. Read the IMO Resolution A.893(21) online: https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.893(21).pdf.

- These data elements are required to be compliant with said authorities, allowing the port master and vessels to enter ports or begin cargo operations. These data elements have a strong impact on safety, as the port master should spend most of his or her time on the bridge rather than completing numerous administrative requirements, which need to be returned to the ship agent, who then processes the data into an application (a PCS, for example) or into hard copy forms. The data also have a strong impact on environment, as timely clearances of authorities helps ensure smooth transit of both ships and their cargo.

- The most robust standardization body for these data elements is the 174-member FAL Committee, together with ISO, WCO, and UNECE, who have been working on FAL forms since standards were first introduced. Therefore, a submission to this standardization body was required to define these data elements and to include the time stamps required both for clearances to realize real-time data exchange between ship, authorities, and supply chain. This submission was approved in the most recent FAL Committee meeting (no. 44).

The most robust standardization body for nautical data elements is the 174-member FAL Committee, together with ISO, WCO, and UNECE

68. ***The priority list of operational data includes three data elements necessary to (a) plan arrival and departure times at berth and at pilot boarding place, as well as (b) starting and completion times of cargo and ship services, including (c) clearances required by the International Ship and Port Facility Security (ISPS) Code.***

- Port planning for an arriving or departing ship is normally organized by the port authority, based on the berth planning of

the terminal in their port area. Port planning tells which ship is welcome at a specific pilot boarding place or which ship can leave from a specific berth, based on maximum vessel sizes, maximum conditions (weather, tide), availability of fairway, and nautical services.

- These data elements are necessary to be compliant with Marine Labor Convention (MLC) and ISPS regulations, and to contribute to the IMO GHG objective of 50 percent emission reduction by 2050. These data elements have a strong impact on safety (rest hour planning), environment (JIT arrivals), and security (ISPS, avoiding piracy areas). Because these data elements are also used for completing notifications and declarations, common sense indicates they should be developed under the same body (FAL Committee) and then built on an existing work. Therefore, at the most recent FAL Committee meeting (no. 44), a submission to this standardization body was made—to expand their scope to include operational data and defining data elements for ship services.

69. ***The problems of data interchange should not be underestimated, and requires equivalency, willingness, and capacity.*** Three issues in particular should be noted:

- First, data owners in the ship–port interface in general have limited information technology (IT) resources and could be lacking an understanding of what data is required and in which format, as current digitization of the ship–port interface is in the early stages, even in ports in developed countries.

- Second, guidance per data set is needed, allowing data owners to understand where and how to start in a step-by-step guide. IMO cannot enforce the use of standards in national waters; however, they can provide nonmandatory instrumental guidance, referencing to industry standards. Development of such guidance has been proposed to FAL Committee during the most recent meeting (no. 44). First examples of such guidance include the Just In Time Arrival Guide[15] published by the IMO GIA to support low carbon shipping and the Port Information Manual,[16] published by the International Taskforce Port Call Optimization (ITPCO) project.

- Third, apart from guidance, data owners also need incentives. Again, the IMO and industry can work together on, for example, the publication and certification of data owners who have implemented the standards for the minimum set of data elements.

NOTES

15. The Just In Time Arrival Guide: Barriers and Potential Solutions, written by GEF-UNDP-IMO GloMEEP Project and members of the GIA and published by IMO in 2020, is available online: https://wwwcdn.imo.org/localresources/en/OurWork/PartnershipsProjects/Documents/GIA-just-in-time-hires.pdf.

16. Read the Port Information Manual, published in 2019 by the ITPCO project, online: https://portcalloptimization.org/images/Port%20Information%20Manual%201.4.4%20-%20final%20%282%29.pdf.

3.3.3 Port Community Systems

70. ***A PCS is an electronic platform connecting the multiple systems operated by a variety of public and private stakeholders that comprise a seaport or airport community.*** Port community systems play a major role as ports and countries move towards the single-window environment, and have a long tradition in Europe, having been first established in ports in Germany, France, and the United Kingdom in the late 1970s or early 1980s. Ports in countries such as the Netherlands and Spain established their port community systems in the 1990s or early 2000s. While in the last decade, the port authority of Cotonou, Benin, established the first PCS in Sub-Saharan Africa, and received the "Gold IT" award in recognition of its successful implementation and operation at the 28th World Ports Conference held in Los Angeles in May 2013. The PCS at the Port of Cotonou has helped reduce dwell time from more than 39 days in 2011 to an estimated 6 days in 2012 and reduced paper consumption by more than 1 million A4 paper sheets per annum.

71. ***The current environment, along with the advent of COVID-19 pandemic—with its greater emphasis on the need to improve digitalization of ports—underscores the potential contribution of a PCS.*** This is summarized in the following statement from Port of Los Angeles:

> "The COVID-19 crisis has provided an opportunity for ports around the world to assess how technology can improve our public health response and support economic recovery. We have to accelerate our efforts. At the Port of Los Angeles, we have been working on this port community system, the only one in the United States, for four years. I have called on the federal government to adopt a nationwide port community system. We have learned so much from our colleagues in Europe, Asia, and the Middle East. It is time to enable that technology in the United States. As the economy begins to re-emerge, data is going to drive our supply chain partners and us toward greater success."
>
> **Gene Seroka**
> Executive Director, Port of Los Angeles

WHAT IS A PORT COMMUNITY SYSTEM?

72. ***The International Port Community System Association (IPCSA) defines "port community system"[17] in the following way (further illustrated in figure 3.3):***

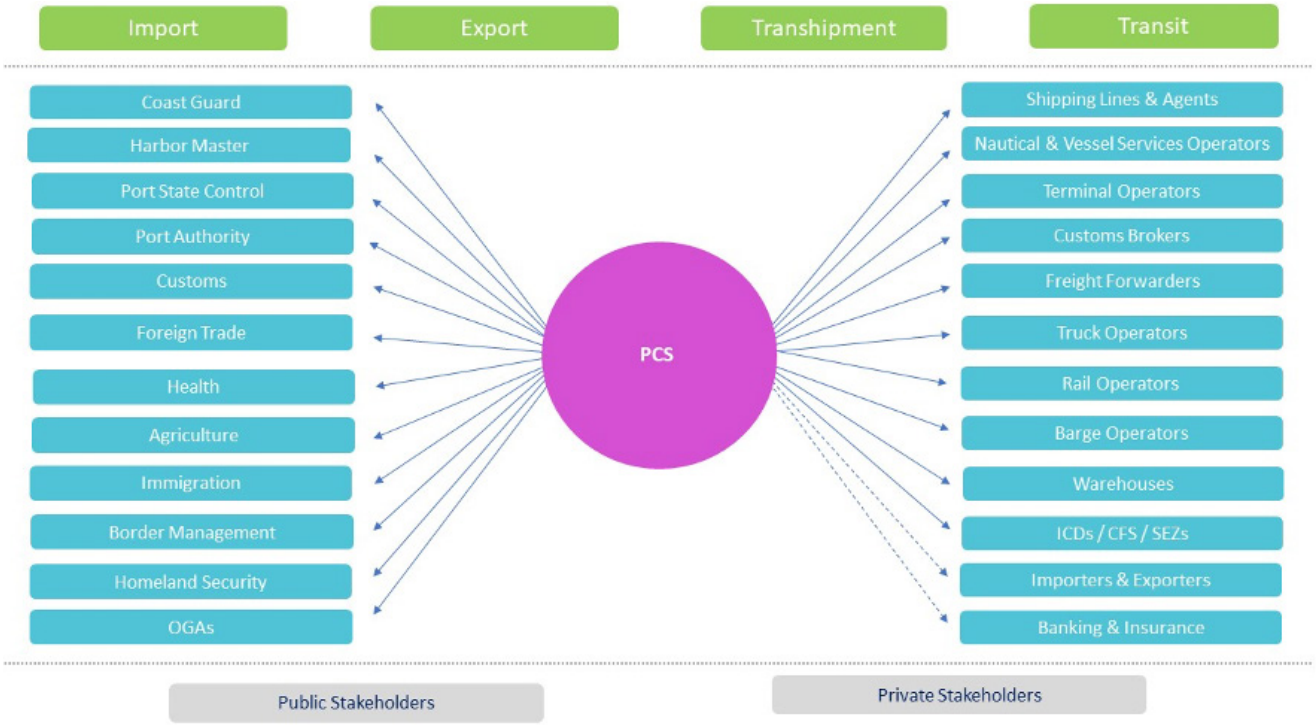
- a neutral and open electronic platform enabling intelligent and secure exchange of information between public and private stakeholders in order to improve the competitive position of the sea and air ports' communities

- optimizes, manages, and automates port and logistics processes through a single submission of data and connecting transport and logistics chains

NOTE

17. Learn more about the IPCSA and its work with port community systems online: https://ipcsa.international/pcs.

Figure 3.3. Port Community System



Source: Figure based on information provided on the IPCSA website (https://www.ipcsa.international/pcs)

73. ***A PCS is then a modular system with functionality designed to provide all sectors and players within a port community environment with tools specific to their needs, thus delivering a tightly integrated system.*** Developed for port users, in most cases by port users, a PCS encompasses the process flows of maritime and air related to exports, imports, transhipment, consolidations, hazardous cargo, waste disposal, crew and passenger reporting, terminal operations, hinterland operations, inspections, voyage notifications, and statistics reporting. Note it does not cover the responsibilities related to the management of the port, which would require a broader system, known as a port management system, which is discussed in chapter 4.

74. ***In general, port community systems provide a wide range of services and key features, which can be summarized as follows:***

- Easy, fast, and efficient EDI information exchange and centralization, available 24/7/365
- Customs declarations, including inspections
- Electronic handling of all information regarding import and export of containerized, general, roll-on/roll-off, and bulk cargo
- Status information and control, tracking, and tracing through the whole logistics chain
- Processing of dangerous goods
- Processing of maritime and other statistics

Port community systems can also facilitate trade and act as gateways into single windows, or in some cases act as the single window for a country

WHAT ARE THE BENEFITS OF A PORT COMMUNITY SYSTEM?

75. ***The core benefits provided by a PCS include higher efficiency and speed regarding port processes, particularly through the reduction of paperwork.*** The functionality is aimed at eliminating unnecessary paperwork—which can clog up cargo handling—and streamline processes through an integrated system. Using electronic data exchange, the PCS is an effective real-time information system: fast, focused, flexible, and multi-faceted, with the main objective of optimizing current supply chain processes by improving operational efficiency and establishing data exchange standards to develop transparency at all stages of cargo handling, including vessel discharge and loading, customs clearance, port health formalities and delivery in and out of the terminal. In this way, port community systems contribute to sustainable transport logistics and support the ambitions to meet global carbon reduction requirements. A PCS also offers improved security, cost reduction, and potentially more competitiveness for each user, as illustrated in table 3.1.

Table 3.1. Benefits of Introducing Port Community Systems

Port community system benefits in Ukraine	Port community system benefits at the Port of Los Angeles	Port of Barcelona: Gate exit	Port of Shanghai e-logistics community system benefits
20% — increase of cargo traffic through the ports of Ukraine in 2019 **1,426** — organizations that joined the IPCS as of April 2020 **2.5 hours to handle cargos and vehicles** in the seaports—down from 15 hours before PCS 15 minutes to register the ships call to the ports of Ukraine controlling bodies—down from 3 hours before PCS **11 documents** submitted by an agent—compared to 53 before PCS **Ranked third** (by the ICC) in the "Fight against Corruption" in the European region	**Cargo visibility:** Increase from 2 to 14 days prior to vessel arrival **Productivity:** 8–12% projected productivity increase as solution is scaled across the Port of Los Angeles **Ease of use:** 93% of pilot participants agree that the data in the portal are easy to understand and valuable **Recent awards:** • American Association of Port Authorities • 2017 Outstanding IT Project Award L.A. Digital Government • Digital Innovator Award, GE Digital	Document checks while exiting container terminals at the Port of Barcelona took at least 3 minutes per truck. Trucks were required to stop and have documents checked to ensure the container was cleared to leave the terminal, including customs clearance **Benefits:** In 2019 the Port of Barcelona partnered with Portic to implement the new PCS-enabled electronic procedures, creating an automatic customs control of departures. Portic has saved transport companies more than 50,000 hours of waiting time at terminal exits	Port of Shanghai e-logistics system evolved from a container terminal operation system (TOPS-C V1.0, 2010) to a fully functioning PCS serving government agencies (such as customs, inspection, and maritime bureaus), shippers, and logistics service providers, including hinterland terminals (TOPS 5.0, 2015) **Benefits:** 75% of document exchanges are electronic; 80% load rate of domestic heavy container trucking; 12% efficiency improvements of tire gantry crane operation; 4,000-ton reduction of annual diesel consumption; and US$60 million annual savings of operating cost
Source: UN Global Compact Network Ukraine. 2020. Voluntary Business Progress Review of Achieving SDGs in Ukraine. https://sustainabledevelopment.un.org/content/documents/26294VNR_2020_Ukraine_Report.pdf	Source: Port of Los Angeles website (accessed October 2020): https://www.portoflosangeles.org	Source: Port of Barcelona website (accessed October 2020): http://www.portdebarcelona.cat/en/home_apb	Source: Study data

76. More detailed examples of port community systems and their benefits for the wider port and hinterland community as well as for government organizations and border agencies, are shown in appendices 1 and 2.

PORT COMMUNITY SYSTEMS STREAMLINE THE CLEARANCE PROCESSES AND FACILITATE TRADE

77. ***Ports are essential nodes of supply chains at any geographic scale.*** Supply chains handle very differentiated products—such as dangerous goods, products of animal origin for human consumption—and, to protect consumers, governmental agencies must subject these goods to different controls, usually on aspects related to the rules of trade, quality, and safety. Many controls could be carried out in different points in the supply chain, though traditionally most have been carried out in ports. The various controls are generally undertaken by public agencies reporting to appropriate line ministries, which can make coordination difficult. In many cases, a prevailing authority is determined, generally the customs service, which will coordinate controls and avoid unnecessary complications and delay. However, in order to apply this type of solution, advanced information on the consignment, along with the status of the respective controls, must be provided to all relevant public agencies. Ports need to do everything in their power to expedite the flow of goods and to minimize the cost of such flows, and to that end should provide digital solutions such as a PCS to share the information, coordinate border services interventions, and avoid unnecessary delay and cost.

78. ***Port community systems can also facilitate trade and act as gateways into single windows, or in some cases act as the single window for a country, subject to its mandate.*** The WTO TFA[18] was the first agreement concluded at the WTO by all members. The agreement entered into force on February 22, 2017, when the WTO obtained the two-thirds acceptance of the agreement from its 164 members. The TFA contains provisions for expediting the movement, release, and clearance of goods, including goods in transit. It also sets out measures for effective cooperation between customs and other appropriate authorities on trade facilitation and customs compliance issues. The agreement aims to help improve transparency, increase possibilities to participate in global value chains, and reduce the scope for corruption. PCSs support the implementation of the TFA through the optimization of data exchange for business-to-business (B2B) and business-to-government (B2G) processes (see figure 3.4).

79. ***The TFA contains reference to UNECE Recommendation No. 33, which is part of the list of trade facilitation measures developed by UNECE over the past 40 years.*** These recommendations reflect best practices in trade procedures and data and documentary

NOTE

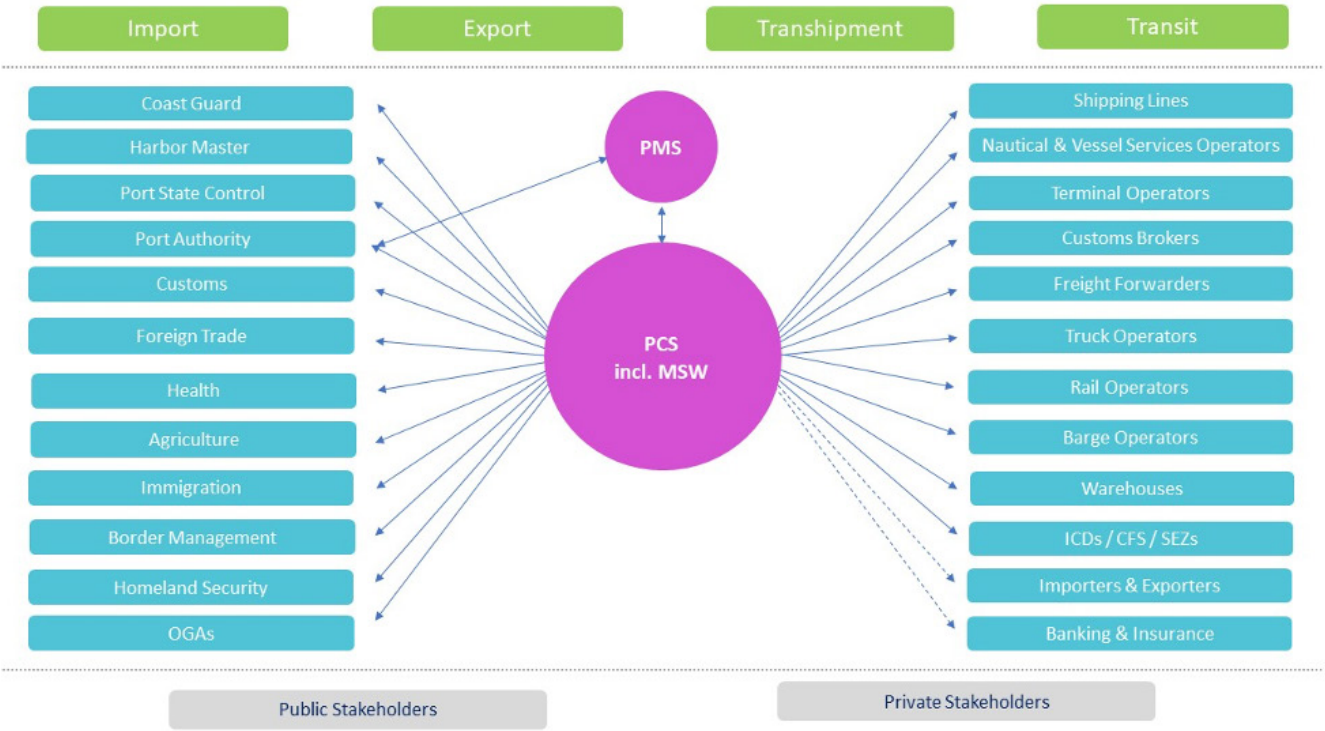
18. Access the World Trade Organization's (WTO) Trade Facilitation Agreement (TFA) online: https://www.tfafacility.org/trade-facilitation-agreement-facility.

requirements, and are used to simplify and harmonize international trade procedures and information flows. Specifically related to this are the suite of UNECE recommendations on single windows—recommendations 33 through 37,[19] which cover single windows, data simplification and standards, legal framework, interoperability and single submission portals. PCSs fall primarily within the single submission portals recommendation, though some, if not all, contain aspects of the other single window recommendation.

NOTE

19. Read the United Nations Economic Commission for Europe's (UNECE) Trade Facilitation Recommendations online: http://www.unece.org/uncefact/tfrecs.html.

Figure 3.4. Port Community System: Optimal Architecture



80. ***However, as the trade facilitation agenda moves forward, several single window initiatives are taking shape in different parts of the world.*** As a result, it is challenging to estimate the number of current operating systems, due to the differentiated single window models adopted and the extent of cross-border operations and functions performed. In most cases customs administrations have a pivotal role in implementation and operation of single window systems across all six WCO Regions. The WCO, through their Building Single Window Environment (SWE) tool,[20] have developed material that assists customs organizations in supporting cross-border trade. Similarly, the IMO has crafted guidelines for an MSW and in April 2019, the FAL Committee issued revised guidelines for setting up an MSW, as

NOTE

20. Explore the Building Single Window Environment tool on the World Customs Organization website: http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/single-window-guidelines.aspx.

detailed in Circular FAL.5-Circ.42,[21] to serve as a source of information, advice, and guidance for those member states looking to create an MSW and provides examples of the experience and knowledge gained by some member states in approaching MSW implementation.

81. ***However, while intergovernmental organizations such as the WTO, UNECE, WCO, and IMO focus—in respect to trade facilitation—in regards to the regulatory aspects of cross-border trade they generally miss the operational aspects such as the physical movement of goods and B2B processes, critical to ensure a seamless movement of cross-border trade.*** Port community systems provide that vital operational information and act as gateways for the trade into single windows. The IPCSA, in its previous European role, issued a publication titled, "Port Community Systems as Gateways to National Single Window."[22]

PORT COMMUNITY SYSTEMS FACILITATE THE SUPPLY CHAIN AND HINTERLAND CONNECTIONS

82. ***Ports also function as modality exchange nodes, where maritime transport, road, barge, and rail transport converge.*** The management of the maritime traffic requires a considerable amount of effort. In addition, the ports must manage properly the negative impact of their operations on the landside, such as long queues of trucks waiting in ports before they can collect their cargo or containers. Some ports have implemented an appointment system, which increases the reliability and efficiency of landside operations. These systems are frequently complemented with IoT sensors at port entry gates and all the information gathered is combined with AI to predict road traffic in the port vicinity to better manage traffic in and out of the port. Thus, a PCS lies at the heart of the system required to ensure ports operate effectively.

83. ***Many ports are looking to strengthen their competitive positions by extending to the hinterland.*** Often, ports and some port terminals promote inland terminals connected via rail, road, and barge to and from their maritime port. Inland terminals offer services similar to those offered by maritime terminals and port community systems facilitate the interconnection between both areas and give access to those services. At the same time, PCSs extend the traceability of the supply chain from port to the hinterland, and vice versa. Multimodality solutions are promoted for cargo transport from and to seaports, to reduce the congestion and improve efficiency in the port area. Consequently, PCSs play an essential role in timing and scheduling of multimodal transport solutions.

NOTE

21. To learn more about the IMO's work in electronic business and access the download link for the April 2019 Guidelines for Setting up a Maritime Single Window (Circular FAL.5-Circ.42), visit: https://www.imo.org/en/OurWork/Facilitation/Pages/ElectronicBusiness-default.aspx.

22.Read the IPCSA white paper, "The Role of Port Community Systems in the Development of the Single Window," published in 2011 when IPCSA functioned as the European Port Community Systems Association (EPCSA): https://ipcsa.international/armoury/resources/epcsa-white-paper-pcs-and-sw-june-2011.pdf.

HOW SHOULD A PORT AUTHORITY DEVELOP AND IMPLEMENT A PCS?

> A port community system is not an IT project, but a change management project.

Javier Gallardo
Portic (IPCSA)

84. ***In 2015, the IPCSA published a guide, How to Develop a Port Community System (IPCSA 2015), which identified twelve key steps to establish a PCS.*** The guide illustrates for organizations—whether they be sea or airport authorities, customs authorities, government departments or agencies, or users of sea, air, and inland ports—the key steps, or actions, in developing a PCS suited to the environment in which they operate, while solving business bottlenecks or delays that create inefficiencies at sea, air and inland ports (see figure 3.5).

Figure 3.5. Port Community Systems: The Twelve Actions

85. ***In addition to the twelve actions, five additional factors should be considered when developing a PCS.*** These include (a) human capital, (b) governance and operating models, (c) international standards, (d) technology considerations, and (e) ongoing development and maintenance. Each factor is discussed in the following paragraphs.

86. ***One of the most crucial factors in the implementation of the PCS is human capital and community engagement.*** Generally, around 40 types of stakeholders could use the PCS services; these stakeholders would then form the port community. The PCS serves entities such as government agencies (customs, border agencies, phytosanitary authorities, for example), trade (shipping lines, freight forwarders, agents, trucking companies, customs brokers, shippers, importers, and others), terminals, port authorities and the services they provide, such as vessel traffic management. These represent only a few examples of the stakeholders involved, and during the development stage a mapping of all stakeholders lays a crucial foundation for developing a successful PCS.

The performance of the port community systems largely depends on the capacity, collaboration, and participation of the port community members

87. ***Human capital is the biggest barrier to development, implementation, and sustainable operation of a successful PCS.*** The performance of the PCS largely depends on the capacity, collaboration, and participation of the port community members. These collaborations, whether physical, informational, or financial, are interdependent and thus create many coordination dependencies. Therefore, change management, incorporating strong stakeholder engagement, is essential to ensure the success of the development process.

88. ***Selecting optimal governance and operating models ensures the sustainability of a PCS.*** If the governance or operating model is wrong, system failure is likely. However, the selection of the optimal model can be challenging, as it depends on the culture, environment, and even politics associated with the port and the country itself. The key criteria for the governance and operating models are neutrality and trust. A PCS needs to be a neutral and trusted third party; if it is not considered trustworthy or neutral, the likelihood of failure increases. In terms of ownership, three main options include the following:

- **Private ownership:** This is a bottom-up approach, in that the private operators such as shipping lines, terminal operators, freight forwarders, brokers, and others own and operate the system. Privately owned systems are easy to implement and are more

flexible in their operations; however, they are still connected to government agencies, including customs, to effectively combine B2B and B2G processes for the benefit of the entire community. Some major ports, particularly in Europe, such as Maritime Cargo Processing plc (United Kingdom), and dbh Logistics and DAKOSY (Germany), adopt this approach.

- **Public ownership:** Port authorities are instrumental in the development of PCS and in many countries they are also the main shareholders. In countries with proactive participation of national public authorities, public ownership models are quite prevalent—for example: Portbase Rotterdam (the Netherlands); Polski PCS (Poland); ePuertoBilbao (Spain); Port of Trieste (Italy); Port St. Maarten (Caribbean); Djibouti PCS (Djibouti); and Port of Antwerp (Belgium).

- **Mixed public-private partnership:** The mixed public-private partnership program aims to achieve a full acceptance and/or an active participation of private companies in top-down PCS implementation. These mixed systems could vary in type and extent of involvement of various stakeholders and can range from a public-private partnership PCS with SOGET and MGI (France) to national trade single windows that incorporate PCS, such as Portnet (Morocco), SEGUCE RDC (Democratic Republic of Congo), and SEGUCE TOGO (Togo), to concessions for services, such as Portic (Barcelona).

The development of any port community system should be based on accepted international standards. There may be more than one required standard and the PCS acts as a translator from one standard or format to another.

89. ***In terms of the operating models, key decisions include whether it will be provided free or a fee will be charged, who will pay, and what type of services will be offered.*** The level of capital costs and the source and level of operating costs must also be considered. The answers to these questions and others will be very much context specific, and depend on the local environment and ownership model, and need to be agreed between all stakeholders, ex ante, or early in the process.

90. ***The development of any PCS should be based on accepted international standards.*** There may be more than one required standard and the PCS acts as a translator from one standard or format to another. Therefore, a review of standards used by the industry and the government agencies will ensure that in any development of digitalization, the process will not place a burden on the trade and other agencies who might need to invest large amounts to change standards. Recommended standards to review include those

developed by UNCEFACT (EDIFACT—messages used by a majority of shipping lines and the multi modal reference data model); PROTECT (messages for port authorities); SMDG (messages for terminals and shipping lines); WCO (customs data reference model); and the IMO FAL reference data model. Traditionally, PCS have exchanged (batch) messages, but as technology moves forward, interfaces such as APIs are being used. This means the underlying reference data models are critical for PCS interoperability with all users, enabling the PCS to translate from one standard to another.

91. ***Creating technology neutral solutions where possible is also recommended.*** Technology should not drive business and processes, but business should assess which processes should be digitalized and what the most appropriate technology should be. This technology neutrality brings the user freedom to choose the most appropriate and suitable technology for the user's need while also standardizing the underlying data. Varying technologies can thus be chosen to lower end costs for users and government agencies and authorities alike. Accordingly, technology-neutral solutions allow a PCS to be future proofed and adapted for ongoing development and maintenance as well as updated efficiently to comply with national and international legislation.

Creating technology neutrality brings the user freedom to choose the most appropriate and suitable technology for the user's need while also standardizing the underlying data.

92. ***Once built, a PCS must be flexible to allow change and adapt to new needs and requirements.*** Possible changes could include updates to local, national, regional, or international legislations as well as to the business trends affecting the movement of goods or the process flow of information. Innovation should also be part of a PCS culture—innovating and adapting not just to technology, but to the greater PCS community and user requirements as well. Just because a PCS has worked in the past and is working now does not mean it cannot be improved or simplified. Box 3.2 highlights the challenges facing many smaller ports in setting up viable and adaptable port community systems.

Box 3.2

Box 3.2. The Challenges Facing Small- and Medium-Sized Ports in Establishing PCS

Even prior to the COVID-19 pandemic and the call for action urging ports to accelerate their role as digital nodes in the supply chain, some smaller and medium-sized ports were actively considering, developing, implementing, and, in some cases, already operating port community systems.

Although the principles of a PCS are the same for every size port, in the Caribbean, Indian Ocean, and Pacific, some small islands have been successfully implementing PCS for the past two decades. However, some smaller ports could have different drivers and varying levels of financial resources and human capital available to develop and operate a PCS. They may face additional challenges in the smaller ports (particularly in the Smaller Island Developing States) in terms of the quality of the internet and the reliability of the power supply—so while larger ports can more easily enable their operations, improve their efficiency, and enhance their competitiveness through digitalization, other ports struggle to implement the initial steps in designing and implementing a PCS.

One promising avenue currently under discussion is the development of a suitably modular PCS, based on open source software, which can be tailored to meet the context and needs of the smaller ports.

Source: IPCSA 2020

REFERENCES

European Commission. 2020. "Cleaner Air in 2020: 0.5% Sulphur Cap for Ships Enters into Force Worldwide." Press Release, January 3, 2020. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6837.

Green Port. 2019. "Ports Seize Opportunities Presented by Drones." September 27, 2019. https://www.greenport.com/news101/energy-and-technology/ports-seize-opportunities-presented-by-drones.

IPCSA (International Port Community Systems Association). 2015. "How to Develop a Port Community System." https://www.ipcsa.international/armoury/resources/ipcsa-guide-english-2015.pdf. Alternate URL: https://www.ipcsa.international/how-to-develop-a-port-community-system.php.

---. 2020. "IPCSA Guidelines on Port Community Systems for Small and Medium Sized Ports." June 26, 2020. https://www.ipcsa.international/armoury/resources/ipcsa-pcs-for-sm-sized-ports-final-published-26-06-2020-1.pdf.

Link-Wills, Kim. 2020. "Port of L.A. Leader Calls for Industrywide Digital Transformation (with Video)." Freight Waves (podcast), September 16, 2020. https://www.freightwaves.com/news/port-of-la-leader-calls-for-industrywide-digital-transformation?p=292251.

PPA (Philippines Port Authority). 2020. "PPA Launches COVID-19 Contact Tracing System for All Port Users, Community ." Press Release, September 19, 2020. https://www.ppa.com.ph/content/ppa-launches-covid-19-contact-tracing-system-all-port-users-community.

Chapter 4: The Medium-Term Recommendations

4.1 Introduction

93. ***Chapter 4 presents the next steps and medium-term recommendations in the development of port community ecosystems and the digitization and resilience of the sector.*** These steps include the development and introduction of a port management system (PMS) and the introduction of smart port technologies, all of which improve the resilience of the maritime logistic chain. The equally urgent requirements related to improving digital security are dealt with in chapter 5. "Medium term" is defined here as between 12 and 24 months, a recommended timeline to underline the urgency of the agenda and intended as an aspiration rather than a definitive timeline.

4.2 Port Management System

94. ***A PMS enables the port authority to control traffic and manage port infrastructure in the port.*** As illustrated in figure 4.1, a PMS encompasses the management of port calls, dues, journal, incidents, waste, dangerous goods, planner, cargo, inspections, permits, services, security, and assets in an integrated manner via one system. This covers a far broader agenda than that of a port community system (PCS), as introduced in the previous chapter, which is intended to facilitate movement of the consignment through the port into and from the hinterland. A PMS, which focuses on the regulatory mission of the port authority, includes those tasks as well, while also encompassing all other activities required for the port to function and thus is a major factor in the relative competitiveness of any port.

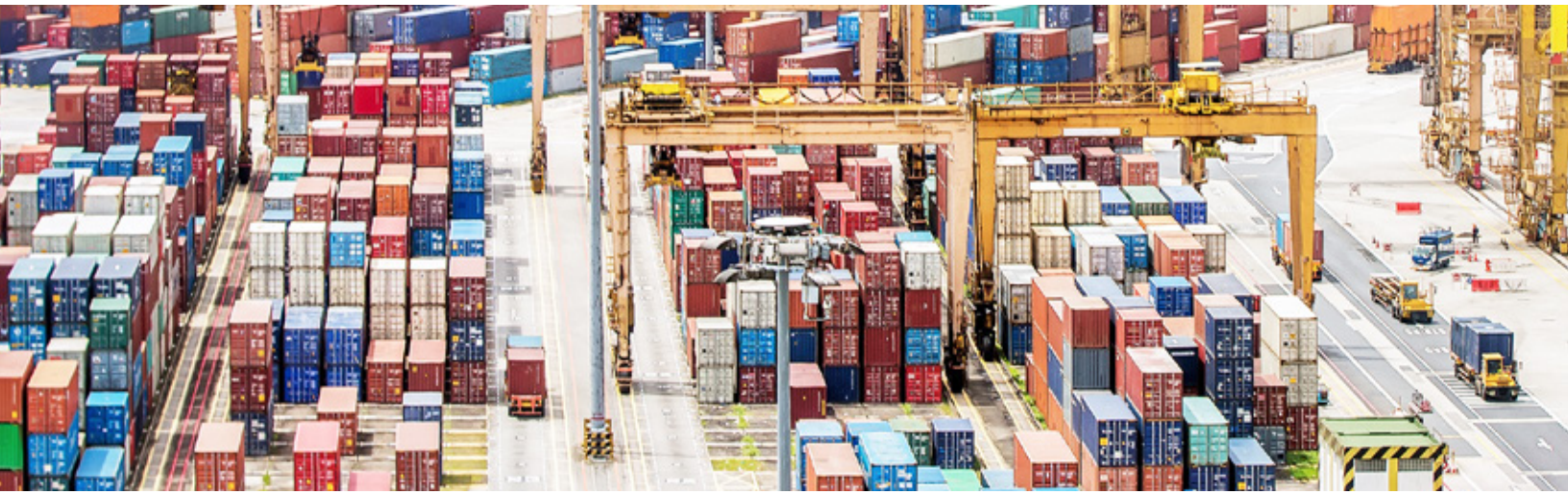
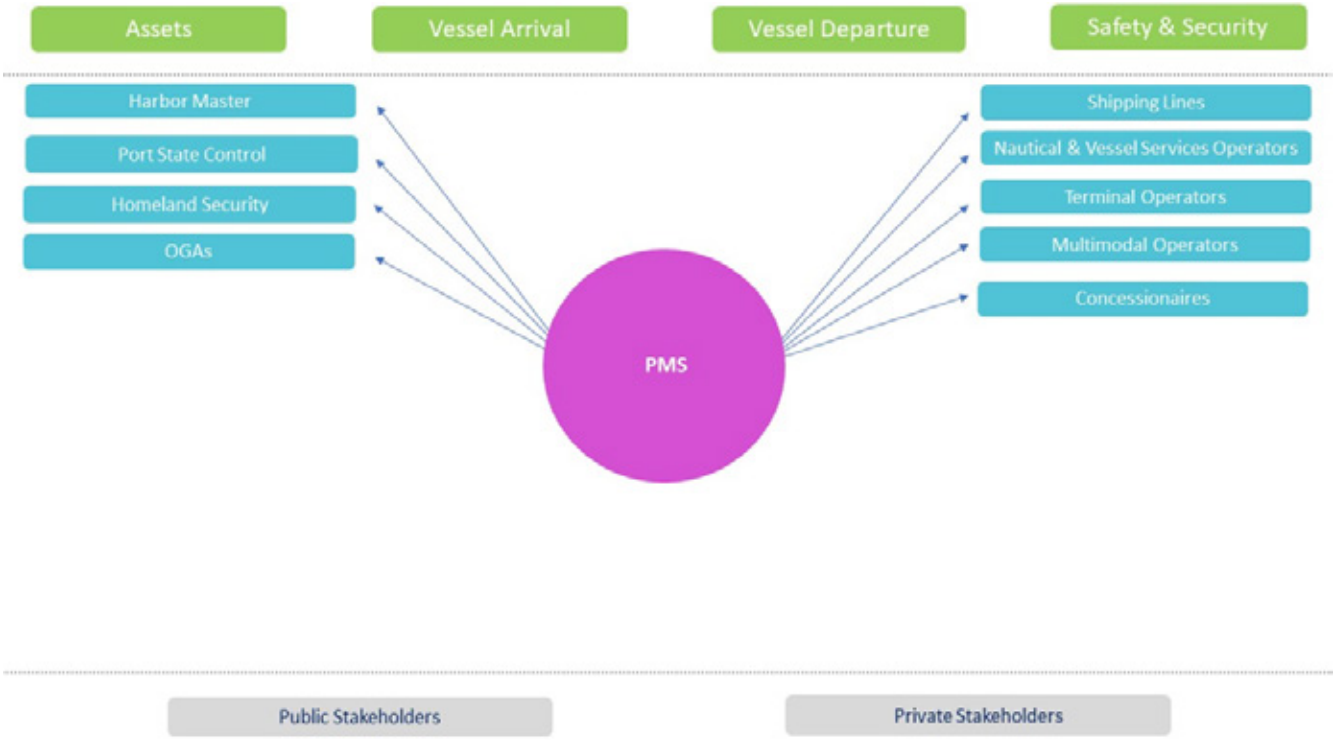


Figure 4.1. Port Management System



95. ***Modern port management requires a performing PMS that supports and enables efficient traffic control.*** In the case of the Port of Antwerp, Belgium, the information technology (IT) department developed the Antwerp Port Information and Control System (APICS). This PMS deals with all relevant aspects of managing shipping traffic to, from, and within the port boundary, including tug activities, lock planning, berth management, and registration of dangerous goods. An intelligent platform, the APICS is the main working solution of traffic controllers, dock masters, quay supervisors, harbor masters, dangerous goods operatives, port dues collectors, tug operators, pilots, Shipping & Signalling Services (SSS), the Agency for Maritime and Coastal Services (MDK), and the shipping police.

96. ***The PMS also assists traffic control in drawing up the optimal planning for vessels arriving in or leaving the port with minimal delays.*** The PMS provides an accurate and actual image of the port and her approach routes, the bridges and locks, and all vessels sailing or moored in the port's working area. All operational events are captured electronically if (and as soon as) possible, minimizing latency. In the context of the Port of Antwerp, the coordinating departments and services have correct, up-to-date information for handling the flow of seagoing ships and barge traffic. The PMS forms the core operating

system as it has to manage more than 35,000 vessel voyages and up to 300,000 barge movements on a yearly basis. With the introduction of the APICS PMS, the Port Authority of Antwerp has moved away from a previous, and rather passive, version of the system focused on recording and monitoring of shipping movements, to an active system in which users are able to optimize their planning processes.

97. ***Ship's agents and forwarders, pilotage and tugging companies, shipping police and customs, port dues officials, and other logistics players in the supply chain all make intensive use of the APICS desk.*** Currently, more than 320 companies use APICS, with about 2,400 active users. Internally, APICS serves as the main tool for vessel traffic controllers, lock operators, dock masters and port state control, harbor masters, and dangerous goods operatives. The system guarantees a smooth, safe, cost-efficient and customer-oriented follow-up of all traffic flows from, to, and in the Port of Antwerp. The APICS system is instrumental to the organization and coordination of all ship movements (inbound/outbound/shifting), lock planning and berth management, and coordination of the dredging operations.

Modern port management requires a performing Port Management System that supports and enables efficient traffic control

98. ***The Port of Antwerp's APICS PMS is connected to various external, public, and private partners.*** A direct linkage between the central broker system hub model and the port's own operational systems means that only one application is needed for uniform communication. This ensures transparency of information and promotes a rapid and up-to-date flow of information. The PMS uses the latest technology to coordinate bridge and lock scheduling with the schedules of various service providers (pilots, tug operators, boatmen, waste collectors, among others). In terms of the regulatory messages, the APICS PMS (the online user interface is called C-Point) is used to convey the following communications (among others), as listed online at: https://www.c-point.be/en/services:

- **Prenotification (seagoing ship)**—used by the shipping company or ship's agent to provide advanced information to the harbor master's office on a seagoing ship due to enter or leave the port.

- **Order for pilot, tug, or mooring services**—used to inform the harbor master's office quickly and easily of any additional services that a ship will need, before it enters the port.

- **Notification of arrival (seagoing ship)**—used by the port authority to notify the customs authorities, via APICS, when a seagoing ship bound for Antwerp actually moors at the berth.

- **Notification of dangerous goods**—used by the ship's agent or freight forwarder to notify the harbor master's office, at least 24 hours in advance, about the position of dangerous goods.

- **ISPS declaration**—submitted electronically by ships wishing to call at an European Union port; under the terms of the International Ship and Port Facility Security Code (ISPS Code), ships must provide certain information to the relevant authorities in the form of an ISPS declaration.

- **Notification of exit (seagoing ship)**—used by the port authority to inform the customs authorities, via APICS, when a seagoing ship unmoors from its berth and leaves the port via the lock.

4.3 The Evolution towards a Smart Port

99. ***A smart port is an automated port that uses nascent technologies such as big data, internet of things (IoT), fifth-generation technology (5G), blockchain solutions, and other smart technology-based methods to improve performance and economic competitiveness.*** With these technologies, smart ports can also improve environmental sustainability. In an ideal smart port, processes would be automated and connected via IoT. This section introduces a smart port technologies use case with a focus on distributed ledger technologies, such as blockchain, digital twin, IoT, 5G, and artificial intelligence (AI).
Distributed ledger technologies: Blockchain

100. ***Blockchain, one of the major Fourth Industrial Revolution technologies, enables real-time tracking and management of logistics activities and asset locations within the supply chain and safe sharing of data among related parties.*** Many ports are now exploring the new business opportunity with blockchain, which could be a game changer for organizing the logistics processes with risk and ownership transfer—without the use of traditional documents, but rather through data sovereignty. Box 4.1 provides an example of the introduction of such technologies in the Port of Busan, Republic of Korea.

Box 4.1

Box 4.1. Example of Blockchain Technologies Implemented in the Port of Busan

The Port of Busan, in the Republic of Korea, is the sixth busiest container port and the second busiest transhipment port in the world (based on 2019 volume). It also serves as a gateway port for Northeast Asia, handling more than 20 million twenty-foot equivalent units (TEU) per year since 2017. The Port of Busan consists of two ports: North Port and New Port, with each port operating three and six terminals respectively.

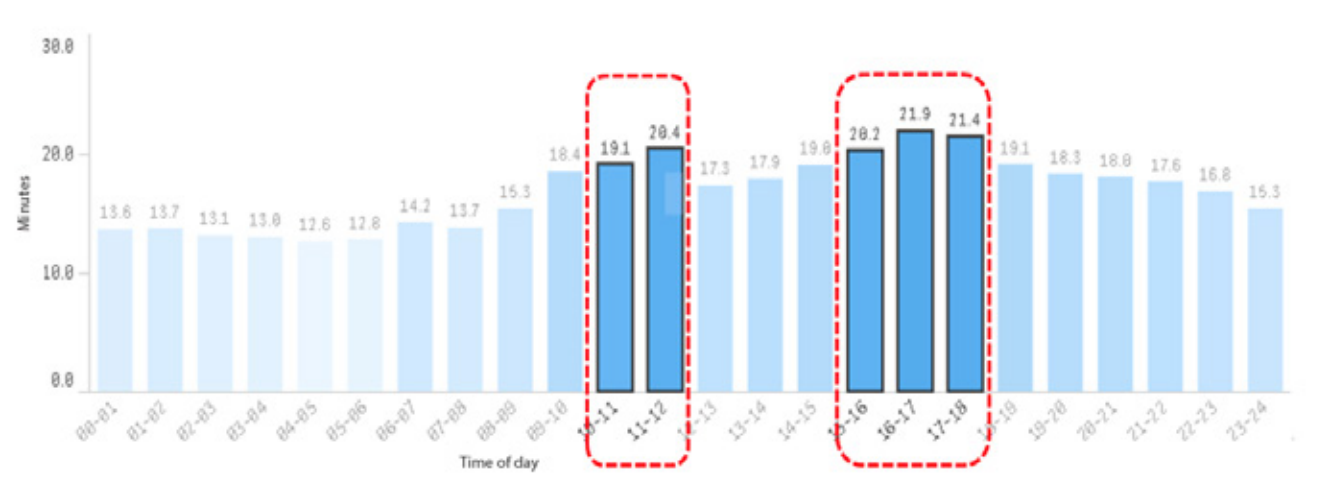
The Development and Future Directions of PCS at Busan Port

The ship arrival and departure work was computerized in 1996 as part of the digital public service system, called **Port–MIS** (management information system). As the first-generation port community system (PCS) in Korea, Port–MIS handled all the port operation and civil service-related works, including arrival reporting, port facility usage, traffic control information, cargo terminal gate-in/out, port dues, and departure reporting, among other tasks in major Korean ports. However, the data accuracy of Port–MIS was inadequate, as it was based on the information reported by shipping lines. When changes occurred in ship arrival and departure schedules, gate-in/out, circumstances, or other operations, shipping lines sometimes omitted or failed to update the modified information in time.

BPA–NET, the second-generation PCS, partially addressed such an issue. It offered improved data reliability by reflecting electronic data interchange (EDI) information into the data reported by shipping lines, and added a function to create statistics generated within the Port of Busan based on the collected data. However, data reliability was still limited, as it relied on faithful, accurate reporting, and there remained an issue created by unintegrated container information. The average truck turn-around time of the terminals stood at approximately 20 minutes (see figure B4.1.1), which was better than other ports in the world in terms of efficiency; however, the lack of accurate data created the following issues:

- Cargo gate-in/out was concentrated at certain times, creating congestion and operational inefficiencies in terminals.
- Longer truck waiting time resulted in fewer containers transported, and not surprisingly, this inefficient use of trucks inevitably led to a decrease in revenue for trucking companies and truck drivers.
- Inefficient truck assignments also led to decreased backhauling and logistics efficiency, increasing trucking cost and creating the need to improve terminal operation efficiency and preserve or increase profits.

Figure B4.1.1 Average Truck Gate-In/Gate-Out Time



Source: Port of Busan, Republic of Korea

Moreover, dispersed data at terminals—due to lack of real-time data sharing between shipping lines, terminals, and trucking companies—led to number of issues, for example: Trucking companies experienced difficulties in allocating trucks, while terminal operators had trouble establishing and operating a yard plan and experienced inefficiencies resulting from a lack of integrated data, such as the length of time needed to verify data errors.

Chain Portal, the third-generation PCS used in the Port of Busan, is based on the real-time data collection made possible with blockchain. It consists of the vehicle booking system, including the interterminal transport system, the integrated terminal monitoring system, and big data, among other components.

Table B4.1.1. Port of Busan: Comparison between Port-MIS, BPA-NET, and Chain Portal

	PORT-MIS	BPA-NET	CHAIN PORTAL
Function	Port operation, civil service	Port operation, civil service, port statistics	VBS, terminal monitoring,big data
Development Year	1996 (1st Generation)	2012 (2nd Generation)	2019 (3rd Generation)
Managed by	Ministry of Oceans and Fisheries	BPA	BPA
Data Source	Reported data (reliant on faithful reporting)	Reported data + EDI	Real-time container status (transfer) information
Data Reliability	Low	Medium	High

Box 4.1 continues

Box 4.1 continues

The major strength of Chain Portal, as compared to the previous PCS, is the use of blockchain (see table B4.1.1), which provides improved work efficiency to stakeholders by increasing data reliability and enabling real-time monitoring of container status. For shipping lines, it provides an environment to improve their work efficiency. Through real-time monitoring of container status and real-time provision of statistics information, shipping lines can respond immediately when container transport-related issues occur. For terminal operators, the system improves terminal operation productivity by allowing them to establish effective workforce and yard operation plans and to minimize container relocation work, all based on the scheduled gate-in/out information (scheduled transport and trucking information, for example). Blockchain is also expected to reduce port emissions by minimizing unnecessary works.

Moreover, the addition of an integrated terminal information search service for trucking companies shortens the time to collect information necessary for vehicle assignment (berth status, container tracking, yard status, and other terminal-related information). The improved search service should reduce transport errors based on the real-time information checking and verification, thus improving the work efficiency of trucking companies. To better serve truck drivers, the underdogs among stakeholders, mobile transhipment (T/S) transport platforms operated separately by each of nine terminal operators were integrated into one platform (reduced from nine platforms to one). This integration will improve drivers' working environment and profit by cutting turn-around time and increasing vehicle turnover rate (figure B4.1.2).

Figure B4.1.2. Mobile Transhipment Transport Platform, Port of Busan

Source: Port of Busan, Republic of Korea

Box 4.1 continues

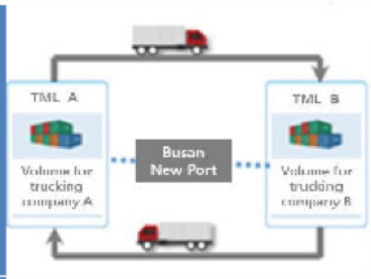
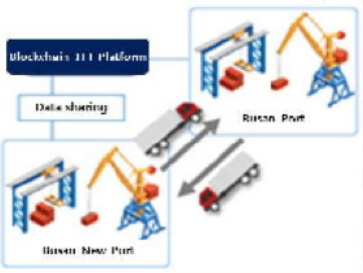
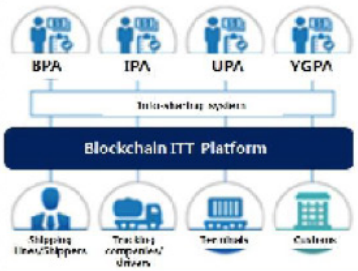
However, the advent of Chain Portal may pose a negative impact on the business model of relay network businesses (value-added network service providers) that have been profiting through Port–MIS. This issue remains to be addressed.

The Introduction of Chain Portal

In 2018, the Busan Port Authority started a pilot project to establish a blockchain platform, with the first phase of Chain Portal beginning in 2019 and ending in March 2020. The project included various systems to enhance vehicle assignment environment, such as a group vehicle assignment system, an integrated terminal information search system, and integrated terminal operator mobile applications.

From August 2020 to February 2021, the second phase of Chain Portal Project will be implemented. The project will include establishment of a vehicle booking system (VBS) and advancement of block-chain-based transport system. After the use of Chain Portal is stabilized in the Port of Busan, it will be applied to other domestic ports in Korea starting from 2022 (see figure B4.1.3).

Figure B4.1.3. Progress of a Chain Portal Project

	1st Phase : 2019~1H 2020 Establishment of Chain Portal	2nd Phase : 2H 2020 Establishment of VBS and advancing Chain Portal	3rd Phase : 2021~2025 Advancement and expanding adoption
Phased adoption of ITT			
Details	-Establishing an information-sharing system for transshipment cargo based on Blockchain. -Establishing ITT group vehicle assignment process to improve efficiency in terminal operation and truck assignment. -Integrating services for both internal and external gates. -Establishing a single window for terminal information search service. -Establishing Open API to invigorate private services. -Establishing a mobile App to improve the working environment of truck drivers.	-Establishing VBS -Advancing Chain Portal(improved functions and integrated with BPA-NET services) -Expanding network by connecting with other Blockchain platforms.	-Stabilization of the system for seamless operation of VBS.(2021) -Expanding to other domestic ports. (2022~2023) -Expanding platform services by connecting to other domestic and overseas ports. (2024~2025)

Source: Port of Busan, Republic of Korea

DIGITAL TWINS, INTERNET OF THINGS, 5G, AND ARTIFICIAL INTELLIGENCE

101. ***Working with scale models has been a common practice during the past century.*** In order to study certain behavior of an original object without examining the original object itself, researchers began building models "to scale," with accurate relationships between all important aspects of the original object. The concept of working with scale models has found its way into many fields, including engineering, architecture, military command, and many others. While each field may use a scale model for a different purpose, to function properly, all scale models are based on the same principles and must meet the same general requirements.

102. ***Today, in the digital era, the fast-evolving gaming industry and the growing computing power have allowed scale models to be developed in a virtual environment, leading to the conception of digital twins.*** As seen in the analog scale models, the digital twin replicates actual physical assets, with the added functionality of integrating processes, people, systems, and devices. Digital twins have three important characteristics: (a) the physical model and corresponding virtual model are connected; (b) this connection is established by generating real-time data from multiple sources, using sensors to represent its near real-time status in working condition or position; and (c) the digital visualization provides both the elements and the dynamics of how an IoT device operates and lives throughout its life cycle. These digital twin system characteristics can be represented in five technical dimensions:

The digital twin replicates actual physical assets, with the added functionality of integrating processes, people, systems, and devices.

- Data and analytics—forming the core of the system
- Visual interface—ranging from simple 2D to full-blown 3D models
- Simulation and physical modeling—replicating the physical model in detail
- Situational awareness—providing real time feed on events happening at a certain location
- Automated systems—ensuring all model processes are automated

103. ***In short, a digital twin is an exact visual copy brought to life by feeding real-time data streams into the model and integrating these interacting streams in such a way that the model comes alive.*** From a port perspective, the advantages of working with a digital twin (see example in figure 4.2, with the digital twin shown at left) are numerous, allowing real-time overview of operations, insight into the actual spatial context, and overall situational awareness when connected with the operational process information.

Figure 4.2. Example of a Digital Twin: Port of Antwerp

104. ***The Port of Antwerp handles a huge amount of digital data.*** Frequently, however, the data take the form of separate systems, with real-time information concerning the port area available to a limited number of users. By integrating all data into one digital twin, nearly all departments within the port community can benefit from the visual user experience, as graphics help users understand complex

situations at a glance. The vessel traffic management information services (VTMISs) are the most obvious users of this digital system; however, the environmental department also uses the visual display of measurements and analysis generated by, for example, the electronic air quality sensors that detect degassing of ships, while the digital twin offers the mobility team a port-wide mobility heat map, and the financial department can generate a one-click graphical depiction of terminal level revenues and port dues.

105. ***A digital twin can be used for real-time monitoring and reporting purposes, and is also instrumental in examining future events.*** The model archives and analyzes past data, which allows event simulation in certain, and programmable, conditions. The Port of Antwerp's digital twin continues to mature as the influx of data gradually increases and is fed into the system. This includes data gathered from windmills, drone air pathways, and automated aerial systems that detect oil spills and emergency situations involving people, such as drowning incidents. In total, more than 90 use cases have been identified for further integration into the digital twin, thereby creating the foundation for a port-wide digital nervous system and the basis for an advanced AI-enabled port management system within three to five years.

Digital twin systems take time to build, so in order to avoid overcomplicating things, the system plan must have the correct basics in place from the beginning.

106. ***Digital twin systems take time to build, and spring from successfully combining existing assets and measurements with new, innovative tools and futureproof technology.*** In order to avoid overcomplicating things, the system plan must have the correct basics in place from the beginning. The first step involves an inventory and analysis of actual data streams to identify the correct and most useful data generated by automated detection and registration. The extended set of geographical information present in the port forms the system's base layer, and includes land use, concessions, pipelines, powerlines, bollards, quay walls, buildings, and so on. The initial phase must have a stable, secure, and automated registration of events in the port environment. Data generated by the PMS or PCS make the ideal starting point, as these systems generate highly relevant and reliable real-time data and are able to feed these data into the digital twin. Other interesting data that could be integrated into the system include weather conditions, status of bridges and locks, and mobility measurements. All these data are very dynamic, contextual, and once integrated into the model they help bring the digital twin to life. Currently, approximately 12 different databases have been integrated via a data lake enabled by an application programming interface (API).

107. ***Another fundamental asset in developing a properly functioning digital twin is the presence of a digital nervous system throughout the port area.*** In Antwerp, a high-performing fiber network allows devices and sensors to connect to the digital twin, either physically or through the air, including cranes, cameras, and traffic lights. By gradually integrating more data into the digital twin, the Port of Antwerp is becoming a digitally futureproof port. In turn, this digitization project is instrumental in reaching higher levels of service and improved operational and managerial efficiency—with a positive effect on sustainability, and a more efficient and economical use of resources and assets. For example, automatic measurement of road surface wear and tear allows better planning of maintenance works, which then helps improve local air quality.

108. ***The presence of a digital nervous system and development of the digital twin have had mutually reinforcing powers, leading to the inception of the Antwerp Port Information and Control Assistant (APICA).*** A digital assistant that combines the skin of the digital twin and the power of integrated data, APICA increases insights into fact-based simulations of operational decisions and their consequences. As they unlock the predictive capacities of the system, the advanced data-analytics and AI functionalities will expand the power of APICA. The combination of multiple real-time data streams will result in a cross-pollination, generating new insights to improve port-area management and development. APICA represents the next step in the Antwerp Port Authority's objective to have a user friendly, fully integrated system managing day-to-day port operations. APICA will provide port authority staff with full situational awareness, as the system will indicate any anomality occurring in the port's ecosystem, and in this way help the Port of Antwerp staff make better and faster decisions.

109. ***The development and rollout of 5G mobile broadband has the potential to not only support, but also accelerate these revolutionary changes.*** Fifth-generation technology presents a variety of benefits over previous generations of wireless connectivity, including greater bandwidth, lower latency, capacity to dedicate resources for critical functions, potential for greatly expanded numbers of devices, and easier sharing of data. In some cases, we see dramatic and exponential gains from previous technologies. Each of these 5G features will have an impact in the transport sector, contributing to transport-specific applications. Of these, three key opportunities present themselves: (a) revolutionary advancements in the potential connectivity of vehicles, (b) an increase in the number and prevalence of connected

5G mobile technology presents a variety of benefits over previous generations of wireless connectivity, including greater bandwidth, lower latency, capacity to dedicate resources for critical functions, potential for greatly expanded numbers of devices, and easier sharing of data.

devices, and (c) improved data availability for transport operations and management. Undoubtedly, digital transport solutions will evolve and entirely new opportunities become more viable in the maritime sector as well as across the wider transport sector.

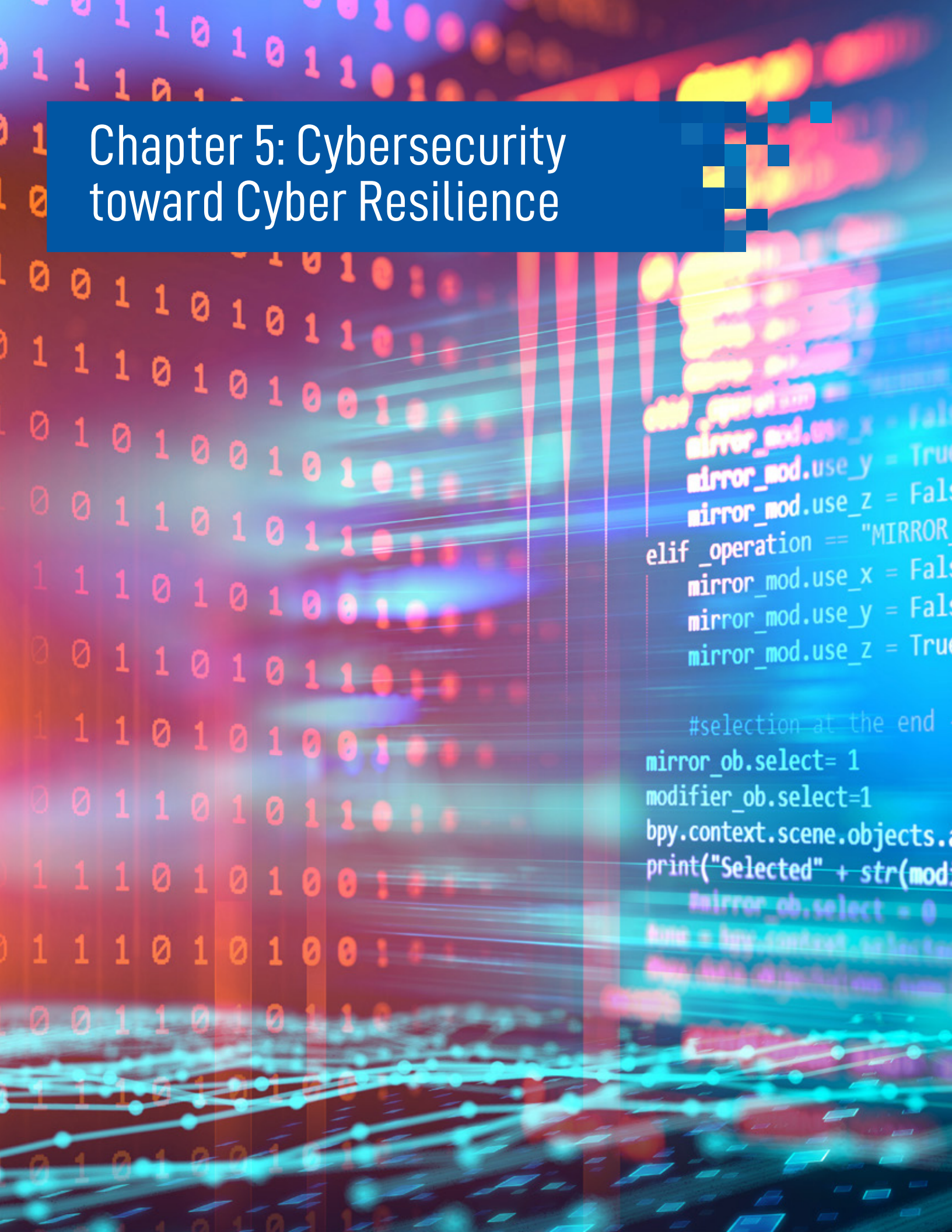
110. ***The 5G technology incorporates three fundamental dimensions for increasing logistics efficiency.*** On the one hand, 5G enables the operation of autonomous vehicles, either by land, by sea, or by air. On the other hand, 5G simplifies many communications and signaling processes, and includes a simplified radio configuration, known as 5G New Radio, which is precisely designed to reduce costs (US$5 per device) and increase device battery life up to 10 years. 5G is specially designed for massive machine-type communications, facilitating the IoT on a large scale. This capacity, within logistics management, will allow for locating all containers, pallets, packages, or other transport units throughout the distribution chain. The on-demand transportation service enabled by this live-tracking of goods and transport unit requires the maximum penetration of third-party logistics (3PL) players, which are typically not well introduced in developing countries. Because of their capacity to adapt their equipment and systems quickly, 3PL should prioritize bringing 5G technologies into the logistics field. Finally, the impact of autonomous vehicles might be seen first in the logistics sector, as long-haul trucking presents one of the simplest and most controlled contexts for autonomous vehicle application.

111. ***In the port sector, two initial 5G tests have been implemented in the port of Rotterdam (the Netherlands) and Bari (Italy).*** The test in Rotterdam focused on the massive deployment of wireless sensors, allowing for real-time monitoring of movement of goods and production of industrial processes in the port. To increase sensor reliability, a 5G network operating at 700 megahertz (MHz) and 3,500 MHz bands in dual band was deployed in the port. The test included analysis of the role of ultra-high definition video surveillance, alongside AI, in detecting and managing cargo loading and unloading. Results indicated maintenance was better predicted, and the additional information allowed inspectors near automatic failure detection. Finally, unmanned robots were used to inspect gas leaks. In addition to making the process safer, substituting the human process with a machine-assisted process increased the inspection's accuracy and reliability.[1]

NOTE

1. The 5G tests conducted in Rotterdam and Bari will be explored further in the forthcoming report, The 5G Enabled Transport Sector, published by The World Bank.

Chapter 5: Cybersecurity toward Cyber Resilience



5.1 Introduction

112. ***In the aftermath of the September 11, 2001, attacks, an overarching emphasis was placed on enhancing physical security capabilities in port facilities and vessels.*** The physical security regulations described within the International Maritime Organization's (IMO) International Ship and Port Security (ISPS) Code further codified minimum protections for port facilities and vessels. While numerous ports hardened their security postures in attaining ISPS Code compliance, the ISPS Code is already outdated in the face of the past decade's explosion of integrated technological advancements. Successfully sustaining effective security in increasingly digitized smart port environments now demands integrating cybersecurity[1] practices into traditional physical security methods.

113. ***Many of the digital developments in the port sector were designed and deployed without considering cybersecurity.*** Port leaders entering the smart port age face increasingly complex decisions regarding investments in new technologies, such as big data,[2] the internet of things (IoT),[3] artificial intelligence (AI), and digital currency exchanges to improve operational performance, enhance automated processes, and increase competitiveness. These capabilities are key building blocks of smart port environments. However, smart ports have an Achilles heel: Many of these platforms were designed and have been deployed without security in mind. In box 5.1, the Port of Antwerp case study illustrates these potential security risks.

NOTES

1. Cybersecurity consists of the collective measures implemented to defend a computer or computer-enabled system against cyber-enabled threats, such as hackers, hacktivists, foreign intelligence services, and organized criminal syndicates, among others.

2. "Big data" is the collection, aggregation, processing, and analysis of various very large data sets to support decision making.

3. The internet of things (IoT) is the system of interrelated computing devices, platforms, and systems that collect and transmit data over networks without human interaction.

Box 5.1

Box 5.1. Case Study: Antwerp—Underscoring the Cyberphysical Security

In 2011, Belgian authorities grew suspicious when containers were discovered abandoned outside the Port of Antwerp. The reason: from 2011 through 2013 a Netherlands-based organized crime syndicate had recruited hackers to breach port information technology (IT) systems that managed container movements. Their objective was to hide narcotics among legitimate cargoes, including containers of timber and bananas shipped from South America. With the hackers' assistance, the criminals accessed the release codes for targeted containers and gained advance knowledge of when and where to send a truck to intercept a container before the legitimate owner arrived.

How did this happen? First, hackers launched a commonly used "phishing" attack, sending innocent-looking malware-infected emails to employees at various terminal operators in the port. Hackers then gained remote access to port data systems and from there accessed cargo management systems and, specifically, container release codes. Although the initial breach was discovered and the malware removed, this did not stop the criminals—who then modified their tactics and physically broke into the port to install key-logging devices on computer systems. Through Wi-Fi connectivity, hackers again gained access to the targeted computer networks, collecting the keystrokes of targeted personnel. The data collected included usernames and passwords to key systems. Using this information, hackers quickly regained access to key systems to continue their smuggling activities. Lesson learned: Traditional investments in supporting ISPS Code compliance did not deliver effective integrated security to port stakeholders.

Source: Port of Antwerp, Belgium

114. ***For port operators functioning in today's IoT-enabled world, ISPS Code compliance does not equate to cybersecurity.*** The IoT's hyperinterconnectedness impacts every port authority, commercial maritime organization, government agency, and individual relying on digital networks, networked systems and applications, cloud-based technologies, and mobile devices. Connected port communities—often serving as the critical foundations supporting entire national economies—are increasingly vulnerable to attack tactics exploiting the vulnerabilities that arise from the integration of digital cyberphysical systems.

115. ***While IoT-enabled technologies offer significant potential operational efficiencies to port stakeholders, they also introduce new vulnerabilities that open the door to cyberthreats.*** The evolution of cyber-enabled platforms, systems, and processes, which are gaining additional momentum with the introduction of predictive analytics software, AI, and IoT devices, is occurring at an extraordinary rate, challenging longstanding security postures. Adapting to such rapid change requires port stakeholders to learn new vocabularies and

terminologies and gain fresh insights into the cyberphysical threat landscape. More importantly, they must understand how cyberphysical threats can impact their organizations, analyze and reevaluate decision-making responsibilities and authorities, employ new training strategies, plan for and prepare to respond to possibly debilitating incidents, and understand how to effectively communicate within their organizations and externally among their port community partners, customers, and key stakeholders.

116. ***In the emerging digital and automated era for ports, commonly termed the "smart port" generation, a growing number of port authorities—with the goal of improving service across supply chains—are coordinating the implementation of new digital technology solutions to deliver connectivity, visibility, and control.*** While digitalization and automation of maritime trade, logistics, transport, and cargo handling have been underway in various guises for many decades now, the trend has clearly accelerated in the past few years and has ramped up substantially during the COVID-19 pandemic. This has consequently increased the cyberattack surface and enticed threat actors. As such, the need for cybersecurity is more vital now than ever. According to London-based company Astaara, there has been a fourfold increase in cyberattacks in the maritime industry since February 2020. The Port of Los Angeles, the busiest container port in the United States, has seen a 50 percent increase in unauthorized intrusion attempts since the beginning of the pandemic. Other ports around the globe also report increased cyberthreat activity.

While digitalization and automation of maritime trade, logistics, transport, and cargo handling have been underway in various guises for many decades now, the trend has clearly accelerated in the past few years and has ramped up substantially during the COVID-19 pandemic.

117. ***Although nearly 10 years have elapsed since the Port of Antwerp attack, it carries wide implications for port communities worldwide, insofar as it represents a convergence of multiple threats, tactics, and paradigms.*** Even more importantly, the lessons learned from the attack remain valid. Key implications include the following:

- ***Convergence of cyber and physical threats.*** This attack involved the coordinated use and combined application of cyber and physical tactics and techniques. The attackers collaborated in their planning, targeting, application, use, and access of key data and information, using the hacked knowledge to assist the physical theft of shipping containers. This represents a critical evolution in the tactics and strategies threat actors are likely to employ against port communities in the future, as threat actors are able to aggressively maintain their persistence over years.

- ***Collaboration of organized crime and hackers.*** The attack resulted from the convergence of a sophisticated organized crime syndicate and technically adept hackers. After the port discovered and mitigated the initial intrusion, the criminals changed tactics and physically broke into the terminal facilities to install snooping devices on administrative computer networks—which represents a cyberbreach—to continue their smuggling operations.

- ***Local law enforcement versus transnational crime.*** Because the Port of Antwerp attack involved multiple terminal operators within a port community, connected to ships, shippers, logistics providers, and various government entities, the vulnerability presented a transnational concern. Since criminals were able to smuggle drugs from South America into the European Union, the vulnerability extended to the entire international trading ecosystem the Port of Antwerp supports, spanning clients, partners, and governments. Integrated cyberphysical threats are pernicious and managing port community risk requires the awareness of all industry stakeholders as well as communication and coordination with relevant local, regional, national, and transnational law enforcement agencies. Collaboration is critical.

118. ***The Port of Antwerp attack illustrates how weaknesses in one area of an organization's security capability can exploit the vulnerabilities that may exist in other areas of an organization's cyber, physical, or electronic security capabilities, and vice versa.*** Because of the converged nature of the cyberphysical risk spectrum, it is crucial that port community leaders consider an integrated approach to planning and implementing digitalized security for their operating environments. Maritime organizations should carefully assess their security capabilities, processes, and internal operations for potential weaknesses and seek to understand how a weakness in one area of the operation might serve as an entry point and subsequent stepping-stone to more sensitive areas.

Because of the converged nature of the cyberphysical risk spectrum, it is crucial that port community leaders consider an integrated approach to planning and implementing digitalized security for their operating environments.

119. ***Further, the Port of Antwerp's experience is not unique, and is not limited to the port, but instead provides a case study reminding port community members they do not operate in isolation.*** Every port community (and its members) operates within the same global ecosystem in which data are regularly exchanged among numerous groups, spanning shipping lines, carrier agents, terminal operators, freight forwarders, road haulage, train operators, border control and inspection, port state control, and customs authorities.

120. ***Port community members make attractive targets for cyberthreat actors in part because so many stakeholders and networks operate within this environment—many with technologies poorly configured against cyberthreats or unsupported legacy systems.*** Cyberthreat actors try to exploit port facilities as a one-to-many cyberthreat vector to port community stakeholders, potentially exposing third parties operating in the terminal environment, including terminal operators, port authorities, customs officials, chandlering companies, agents, vendor representatives, and many others. In this sense, digitalization, which is discussed in chapter 6, brings both the benefits of increased efficiency and the costs of heightened security risks.

Cyberthreat actors try to exploit port facilities as a one-to-many cyberthreat vector to port community stakeholders, potentially exposing third parties operating in the terminal environment, including terminal operators, port authorities, customs officials, chandlering companies, agents, vendor representatives, and many others.

121. ***Increasingly, port facilities are adopting and integrating a broad range of physical and electronic security systems, along with operational technologies—both wired and wireless—to facilitate more efficient and streamlined operations.*** These efforts are giving rise to faster cargo movements through port environments. The more network-enabled devices deployed to this end, the more port communities—and the maritime industry overall—become vulnerable to exploitation by a wide range of cyberphysical (or "converged") threats.

122. ***Locally, port networks need to ensure data are both available and accurate.*** For example, a threat actor gaining unauthorized access to a terminal operating system (TOS) could misdirect cargo container assignments, change bill of lading data to minimize the possibility of customs inspections to enable smuggling, or modify scheduling information to facilitate illicit (but authorized) physical entry to a facility. Compromised video monitoring systems can also be manipulated to deceive security personnel and enable threat actors to gain entry to restricted areas. Such cyberphysical vulnerabilities can lead to ISPS Code failures. Unfortunately, threat actors frequently exploit these vulnerabilities, and the results span business disruption, property loss, loss of life and injury, environmental damage, liability exposure, and reputational damage.

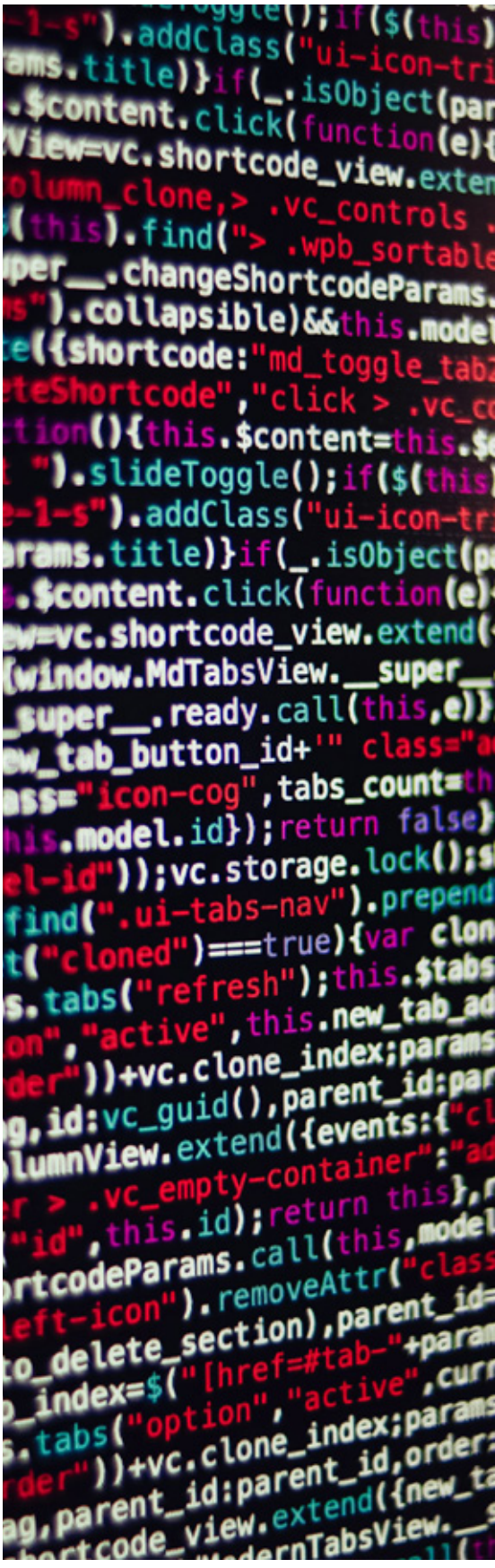
THE CONVERGENCE OF OPERATIONAL TECHNOLOGY, INFORMATION TECHNOLOGY, AND IOT

123. ***One factor driving both the evolution and complexity of cyber-physical threats is the convergence of, and in many cases connectivity among, the following:***

- Information technology-based (IT) systems, such as access control, enterprise resource planning applications, TOSs, and more
- Domain awareness systems, such as closed-circuit television (CCTV), radar, automatic identification system (AIS), and other security monitoring programs
- Operational technology (OT) systems, such as industrial control systems, supervisory control and data acquisition (SCADA)-enabled systems, cranes, conveyor systems, utility infrastructures, and others

124. ***Smart port communities have become progressively reliant on these systems and the IoT devices and platforms that enable business intelligence.*** This business intelligence encompasses the data collected and aggregated to enable operational process improvements, workflow efficiencies, and real-time condition monitoring (asset location, temperature, energy usage, among others) for the purpose of delivering situational awareness to inform decision making.

125. ***However, as more ports and maritime organizations connect these intelligent systems to existing networks, and further seek to adopt and employ IoT technologies—recognizing the corresponding operational efficiencies—new vulnerabilities will emerge that threat actors can exploit.*** In particular, where cyber-enabled systems intersect with electronic, electromechanical, and SCADA-enabled systems, then access control, identity management, inventory control and security systems, cybersecurity, and traditional ISPS-related security vulnerabilities converge.



5.2 Integrated Security Considerations for Port Communities

126. ***Port communities are essential contributors to a country's economy.*** Securing port communities in today's technologically evolving, hyperconnected environment is critical to the host country's economy, the host country's security, and the security of the individual port community stakeholders as well as their global network of trading partners. As required by the IMO's ISPS Code, port facilities must monitor and provide for their own security as well as the safety and security of visiting vessels berthed at their facilities. Antwerp's lessons are clear: Port facilities need to take an integrated approach to implementing and sustaining digitally enabled security in today's threat environment.

127. ***Every port facility needs to develop its own specific engagement strategy around a foundational set of approach considerations.*** As most port facilities must comply with IMO requirements, investments in integrated security should align with compliance needs, but also be designed to accommodate the technological evolution underway in most ports. Additionally, long-term success and sustainability will depend on the utilization of an effective collaboration mechanism (or the establishment of one) prior to or concurrent with initiating an integrated digital security project. Ultimately, tailoring such approach considerations should occur through the development of a core set of guiding principles set forth in section 5.6, The Proposed Approach for Implementation, at the end of this chapter.

128. ***While effective security management is not a compliance-focused mission, it should still consider ISPS Code requirements.*** As discussed at length in Section 1.3.4 of the ISPS Code, port facilities are required to perform port facility security assessments (PFSAs), which inform the subsequent production of a port facility security plan (PFSP). Port facilities subject to ISPS Code requirements must update their existing PFSPs if they deploy new integrated cyberphysical capabilities that result in material changes to the PFSP. ISPS Code elements that affect integrated cyberphysical security and operations include:

- Gathering and assessing of information with respect to security threats;

- Preventing unauthorized access to vessels, facilities, and their restricted areas;
- Monitoring of port facilities, including anchoring and berthing areas;
- Ensuring that security communication is readily available;
- Following procedures for reporting security incidents;
- Maintaining critical operations of port facility and ship–port interfaces; and
- Designing measures to ensure the effective security of cargo (container, bulk, and break-bulk) and cargo handling equipment and storage facilities at the port facility.

129. ***As an international framework, the ISPS Code offers guidance for organizations required to comply with the standards; however, the code does not offer specific, prescriptive guidance on how to achieve compliance.*** Further, the ISPS Code is now 17 years old, and many ports have evolved since the ISPS Code's creation in 2003. Thus, a key challenge is to implement efficient, effective, and appropriate integrated security solutions that support the organization's efforts beyond that which regulations require. In this context, integrated security for port community members includes the physical, electronic, and cyberdefense measures of digitally enabled systems that are integrated with a sustainable blend of people, processes, tools, and funding to counter converging threats.

130. ***Although at the moment the ISPS Code includes relatively narrow cyberphysical security requirements for port facilities, the IMO has begun to take tentative steps toward a more comprehensive approach.*** For instance, with the ongoing challenges imposed on the global economy by the COVID-19 pandemic, the IMO, with leading industry partners, recently acknowledged the extraordinary circumstances that now face the global port community—the national and regional lockdowns and staffing challenges that are resulting in logistics and supply disruptions impacting the world's economy—by calling on the global port community to accelerate the digitalization of maritime trade and logistics capabilities. In Circular Letter No. 4204/Add.20, Coronavirus (COVID-19): Accelerating Digitalization of Maritime Trade and Logistics—A Call to Action,[4] the IMO specifically

NOTE

4. The IMO's call to action for increased digitalization surrounding maritime trade during the COVID-19 pandemic (Circular No. 4204/Add.20, dated 5 June 2020), can be viewed online: https://wwwcdn.imo.org/localresources/en/MediaCentre/HotTopics/Documents/COVID%20CL%204204%20adds/Circular%20Letter%20No.4204-Add.20%20-%20Coronavirus%20(Covid-19)%20-%20Accelerating%20Digitalization%20Of%20Maritime%20Trade.pdf.

includes the establishment of frameworks to enhance port data sharing, standard classification of the critical components—that is, infrastructure and its systems—the expansion of port community systems and their supporting infrastructures, and for members to review the "IMO's Guidance on Maritime Cyber Risk Management[5] on its ability to address cyber risks in ports."

131. ***The IMO Guidelines on Maritime Cyber Risk Management, which are currently in place for shipping companies, emphasize two key points.*** First, cyber risk management efforts should consider IT and OT environments in the context of safety and security.[6] Second, the guidelines directly align with the five functions detailed in section 5.3, Improving Cybersecurity for Port Community Stakeholders. Within the context of the IMO's advocacy for a risk management approach, combined with their co-opting of the cybersecurity framework developed by the United States National institute of Standards and Technology (NIST), it is possible that the IMO will eventually extend its cyber guidelines to facilities via an update to the ISPS Code. As a result, investment strategies for developing integrated digital security capabilities within port communities should consider the possibility the IMO will require port facilities to more fully address their cyber risks.

PORT COMMUNITY COLLABORATION AND INFORMATION SHARING

132. ***Although the Port of Antwerp attack was discovered back in 2013, cyberphysical attacks against port communities and members have continued to increase in frequency and sophistication.*** This presents significant challenges for defending against threat actors who are persistent, well resourced, and operationally nimble in employing a wide variety of cyberphysical tactics, techniques, and procedures to compromise systems, modify data, gain entry to facilities, and jeopardize maritime operations. Given the risks these activities present, it is crucial that port community members share information at the port level, regional level, and sometimes national level to improve their security postures.

133. ***Sharing cyberphysical threat information can help port community members identify, assess, monitor, and respond to a range of threats.*** Mechanisms such as security alerts, suspicious activity reports, and breach of security notifications can facilitate the sharing of multiple types of information among security operations professionals. By exchanging cyberphysical information within a port community, and especially within a port community system environment,

NOTE

5. The IMO's Guidelines on Maritime Cyber Risk Management (Circular No. MSC-FAL.1/Circ.3, dated July 5, 2017) can be viewed online: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf.

6. See the IMO's Guidelines on Maritime Cyber Risk Management, Page 2, Sections 2.1.2 to 2.1.6.

members can leverage the knowledge, expertise, and capabilities of the community to gain better insights into potential threats and make more informed decisions regarding the allocation of security capabilities and resources.

134. ***Information sharing partnerships should be encouraged among port community members, including the captain of the port, local law enforcement, customs, various first responders, and logistics partners.*** If no facility or mechanism exists for information sharing within a port community, the port community should establish a local body to organize and sustain information sharing activities covering cyberphysical security. Such a body can be formed along the lines of a local or regional area maritime security committee, with individual subcommittees tasked for monitoring and sharing cyber and physical threats.

5.3 Improving Cybersecurity for Port Community Stakeholders

135. ***Members of the port community ecosystem can reduce their own cyber risks by implementing essential cybersecurity building blocks such as a cybersecurity framework.*** The five-step cybersecurity framework developed by NIST is one example for reducing cyber risks to critical infrastructure.[7] The framework has become widely accepted as a tool that can help manage and reduce risks related to cyberthreats and focuses on five separate critical functions needed to increase cyber resilience: identify, protect, detect, respond, and recover. In this section, we outline the five functions and what they might mean for a port and a port community:

- **Identify.** The first function of the framework—*identify*—provides a necessary basis for any organization to start or further professionalize their cybersecurity measures. This function serves to understand the business context and critical functions in order to determine the areas where cybersecurity measures should be taken and prioritized. In this first step, the organization should define personnel roles and responsibilities for cyber risk management and *identify* the systems, assets, data, and capabilities that, when disrupted, could pose a risk to the port operators. Box 5.2 provides a case study example for the identify function.

NOTE

7. Learn more about the United States National Institute of Standards and Technology's (NIST) cybersecurity framework online: https://www.nist.gov/cyberframework/new-framework.

Box 5.2

Box 5.2. Function 1 (Identify) Case Study: Rotterdam

The nautical and maritime stakeholders in the Port of Rotterdam performed an analysis of the vital process, "safe and efficient handling of shipping," to determine which systems and partners are vital to the continuation of the process. This analysis resulted in an overview of applications and IT infrastructure used by the nautical and maritime partners. It also identified the interdependencies between these systems. With this analysis in hand, the organizations were able to prioritize a set of measures aimed to ensure the availability and integrity of the process surrounding the safe and efficient handling of shipping.

Source: Port of Rotterdam, the Netherlands

- **Protect:** The second function of the framework—***protect***—includes taking measures such as putting identity and access management in place, to ensure access to data and systems is only granted to those who need it for executing their tasks. This aspect is also relevant to comply with national and international privacy legislation, such as the European Union's General Data Protection Regulation (GDPR). The protect function also focuses on managing protective services such as firewalls, end-point protection, and managing vulnerabilities and patching procedures. Furthermore, ongoing investment in staff training (IT, OT and support) should be made to keep pace with the fast-changing challenges of cybersecurity. Another aspect of the protect function is creating awareness. When professionals discuss cyber resilience, they often refer to people as the weakest link. And indeed, this could be true in breaches that involve phishing, social engineering, or another form of human contact. However, when "working cyber secure" becomes part of an organization's safety and security culture, people may in fact be your strongest link. When employees are taught to detect and report suspicious behavior, emails and changes in IT, they become a robust line of defense. It is therefore vital to invest in ongoing efforts to raise cybersecurity awareness. Also, in the protect phase a risk control processes and measures should be implemented, and contingency planning to protect against a cyber event should ensure continuity of port operations, including awareness on board level.

- **Detect:** The third function of the framework—***detect***—is one of increasing importance. Even though an organization has protective measures in place, it could still suffer from a breach or hack. To prevent or minimize the amount of data loss or damage to the organization's cyber network, breaches must be detected in a timely manner. Benchmark research conducted in 2018 by IBM

The five-step cybersecurity framework developed by NIST is one example for reducing cyber risks to critical infrastructure

Box 5.3

Box 5.3. Function 3 (Detect) Case Study: Los Angeles

The Port of Los Angeles Cyber Security Operations Center employs advanced technologies with layered detection capabilities, which block millions of unauthorized intrusion attempts at the perimeter of the network every month. Within the network, multiple intrusion detection layers continuously detect suspicious activities.

Source: Port of Los Angeles, California

Security showed that on average a breach is detected after 197 days.[8] The same research revealed that the mean time needed to contain the breach was 69 days. Knowing the normal (baseline) behavior of an organization's IT and OT is crucial in detecting potential malicious activities. Box 5.3 provides a case study example for the ***detect*** function.

- **Respond and Recover:** To be able to ***respond*** (phase 4) and recover (phase 5) from a cybersecurity incident, an organization should have identified the need for backup and restore facilities. This can help to decrease the impact of an incident on port operations. The statistics on the lengthy mean time needed to contain a breach show it is critically important to work on incident response and recovery, the final two functions of the NIST framework. Incident response planning and training are crucial to decrease the mean time to contain a breach as well as prevent excessive damage, including reputational damage. The IT incident response team should be ready to act according to a predefined response and recovery strategy, which should include communications departments to ensure appropriate internal and external crisis communications to help protect the organization's reputation. A computer emergency response team (CERT) is an example of a response capability. Vendors may offer this as a service or organizations could decide to set-up an in-house response team by extensively training and educating staff. Board-level awareness is also vital. In the end, the objective of cyber resilience is to reduce risks. The work of cybersecurity professionals contributes to decreasing the risk of comprises to the confidentiality, integrity, or availability of data, processes, and business. Without awareness at the top, an organization's commitment to cybersecurity may result in a mismatch between its cybersecurity maturity and the board's risk appetite. Box 5.4 provides a case study example for the ***respond*** function.

NOTE

8. See the full benchmark research report published by IBM: *2018 Cost of a Data Breach Study: Global Overview*. https://www.ibm.com/downloads/cas/861MNWN2.

Box 5.4

Box 5.4. Function 4 (Respond) Case Study: Rotterdam

The Port of Rotterdam Authority has developed its own cyber crisis response strategy which includes a port crisis team. The aim of this team is to make strategic decisions on the continuation of safe and efficient handling of shipping. The crisis team is supported by three action centers. One center focuses on maritime issues, another on solving the IT issue at hand, and the final center aims to align communication (both inward and outward) between the parties involved.

Source: Port of Rotterdam, the Netherlands

5.4 Cybersecurity Measures for the Port Community Ecosystem

136. ***The European Union Agency for Cybersecurity (ENISA) has recently introduced four cyberattack scenarios at the port community level:***[9]

- **Scenario A:** Acquiring critical data to steal high-value cargo or allow illegal trafficking through a targeted attack
- **Scenario B:** Propagation of ransomware leading to a total shutdown of port operations
- **Scenario C:** Compromise of port community systems for manipulation or theft of data
- **Scenario D:** Compromise of operational technology systems creating a major accident in port areas

137. ***The port community ecosystem, made up of its many individual yet interdependent members, can reduce the ecosystem cyber risks and mitigate these scenarios by working together for port community cyberdefense.*** Working together involves port community members uniting against attacks and collaboratively implementing community cyberdefense strategy, governance, threat information collection and distribution, data use, training and other factors important to the community. Working together does not mean that members share their cybersecurity internal operations or sensitive information with other community members. The benefits of port community cyberdefense include the following:

- **Greater collective knowledge.** Community cyberdefense results in a greater collective knowledge base of the threats against the community. Similar to a traditional neighborhood watch scheme, each community member can now learn about threats they did not see from others in the community who did see, and then shared.
- **Improved resilience.** Port community members depend on each other as goods are moved from one entity to the next within a supply chain. A disruption to one member will have ripple effects, as the recent Shen Attack Cyber Risk Scenario conducted by the University of Cambridge and Lloyd's (Daffron 2019) aptly indicates.

NOTE

9. Read the full report, Port Cybersecurity: *Good Practices for Cybersecurity in the Maritime Sector* published in 2019 by ENISA, available online: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector.

Working together involves port community members uniting against attacks and collaboratively implementing community cyberdefense strategy, governance, threat information collection and distribution, data use, training and other factors important to the community.

Community cyberdefense provides the community with greater resilience, including reducing the risks of supply chain disruptions.

- **Early warning system.** Community cyberdefense provides its members with an early warning of threats against their community. Members could be alerted of threats before the information is made available through other channels.

- **Collaboration forum:** In addition to the technical aspects, port community cyberdefense provides the forum for collaboration among members. Developing a body of knowledge, procedures, and policies for the whole community is paramount.

138. ***To lead this effort, port authorities have been inherently endowed with a natural and neutral orchestration role.*** This can and should be leveraged to facilitate dialogue throughout the whole port community ecosystem and promote a holistic approach that includes not only trade stakeholders, but also city and regional governmental agencies and ministries, including those responsible for national security and defense. Technologies can be a force multiplier for this orchestration to more effectively prevent an attack from propagating to multiple members in the ecosystem that potentially could cut off the flow of goods at a port and disrupt the entire community—and indeed national economies and international trade—by breaking the supply chain.

The Port of Los Angeles has upgraded its Cyber Security Operations Center (CSOC), taking port community cyber resilience to the next level with advanced technologies to automate the orchestration of port community cyberdefense.

139. ***The Port of Los Angeles provides a good example of a port community cyberdefense scheme.*** Several port communities have already implemented various degrees of cybersecurity discussion forums and roundtables in their ecosystem; manual orchestration is a good start. The Port of Los Angeles has upgraded its Cyber Security Operations Center (CSOC), taking port community cyber resilience to the next level with advanced technologies to automate the orchestration of port community cyberdefense. As an integral part of the port's Cyber Resilience Center, the second-generation CSOC will leverage the port's existing cybersecurity operations, along with cyberthreat information from within the port community as well as cyberthreat intelligence from external sources for greater speed, accuracy, and quantity of relevant cyberthreat information to prevent incidents and serve a resource for restoring operations. Box 5.5 describes the Port of Los Angeles's new Cyber Security Operations Center in more detail.

Box 5.5. Cybersecurity Operations Center in the Port of Los Angeles

The second-generation Cyber Security Operations Center at the Port of Los Angeles

The Port of Los Angeles, California, is a global leader among ports on cybersecurity. In 2014, it became the first port in the world to implement a state-of-the-art Cyber Security Operations Center (CSOC). In 2015, it became the first port in the world to attain the ISO 27001 certification, the international standard for cybersecurity. Continuing to advance its cybersecurity program, in 2019 the Port of Los Angeles successfully completed its second-generation (G2) CSOC, shown in the photo.

The G2 CSOC was developed on the original CSOC, but with upgraded technologies, new analytical tools, and the benefit of five years of experience and cyberoperations data to focus the G2 CSOC on the highest priority areas. Today, the G2 CSOC protects the port against more frequent, sophisticated, and damaging attacks, including 20 to 30 million unauthorized intrusion attempts per month.

The next evolution of the port's cybersecurity program will extend beyond the port authority and into the port community with its Cyber Resilience Center, a first-of-its-kind solution to reduce cyber risks in the port ecosystem. The G2 CSOC will be an important component of the port's Cyber Resilience Center by sharing information with the Port of Los Angeles ecosystem for collaboration and engagement with stakeholders, which will result in greater collective knowledge and stronger community defense against cyberthreats.

Source: Port of Los Angeles, California

Box 5.1

5.5 Other Considerations

140. ***When addressing risks to a port community's cybersecurity, the potential financial risks must also be considered.*** According to the World Economic Forum, economic loss owing to cybercrime is predicted to reach US$3 trillion in 2020, representing 3.4 percent of global gross domestic product (GDP) (WEF 2020). In order to develop collaborative approaches and enhance cooperation between their public and private sector stakeholders,[10] port communities must not only initiate but, crucially, expand the cybersecurity dialogue within and between port communities; these conversations must be grounded in financial terms. Doing so translates cyber risk management into the structural conceptions and financial management metrics of port business. Establishing the cyber-risk-to-money intersection across all areas of an organization will offer a means of measurement to inform investment decisions regarding resource identification, allocation and prioritization. Critically, this empowers decision makers with relevant commercial context and the key inputs necessary to make such judgments in a consistent manner.

141. ***To fund investment decisions, some port communities have taken key first steps to drive cybersecurity capability development in their environments by engaging with investors and experts.*** Cybersecurity efforts are rapidly strengthening at key port trade hubs as a direct result of a new wave of investment accelerators, technical centers of excellence, and academic programs focused on innovative technologies, including startups in ports and maritime trade logistics. In 2019 alone, venture capital firms invested an historic US$7.86 billion in 646 cybersecurity startups, and with the emerging information security global market currently estimated at US$120.6 billion, opportunities for technological disruption will continue to expand and grow at an exponential pace. And so too will the cyberthreat landscape continue to evolve. Some of the companies around the world leading these efforts include PortXL in Rotterdam, Dock Innovation Hub in Israel, and Pier71 in Singapore.[11]

142. ***Ports must also take into account considerations surrounding compliance with IMO cybersecurity regulations.*** While each nation has its own unique cybersecurity compliance requirements, this section focuses on security-related instruments directly affecting cybersecurity, which are provided by the IMO, the United Nations global shipping regulator. It is vital for ports, terminals, and port communities to have a clear understanding of how IMO regulates

NOTES

10. See the full summary of the IPCSA workshop held July 15, 2015, in London, UK: "Cybersecurity in the Maritime and Logistics Supply Chain Workshop: Summary, Conclusions and Recommendations." https://ipcsa.international/armoury/resources/ipcsa-cybersecurity-workshop-final.pdf.

11. For information on the three companies working on maritime cybersecurity, as discussed in this chapter, visit the following websites: PortXL (https://portxl.org/) in Rotterdam, Dock Innovation Hub (https://www.thedockinnovation.com/) in Israel, and Pier71 (https://www.pier71.sg/) in Singapore.

cybersecurity in order to embed compliance within the broader aspects of port and port community cyber risk management. The two main IMO regulatory instruments in the context of port security are the International Ship and Port Facility Security (ISPS) Code, part of the International Convention for the Safety of Life at Sea (SOLAS) 1974, as amended in January 2020,[12] and the International Safety Management (ISM) Code, which has been extended by Guidelines on Maritime Cyber Risk Management.[13] The Code of Practice on Security in Ports,[14] developed jointly by the International Labour Organization (ILO) and the IMO, is also important in this respect.

143. ***The IMO's ISPS Code, as part of the SOLAS Convention, is a comprehensive mandatory security regime for international shipping and port facilities.*** The ISPS Code aims to provide a standardized, consistent framework for evaluating all security risks, enabling governments to ensure that proportionate security measures are implemented. The ISPS Code focuses on threats posed to maritime security and more specifically, to certain categories of international shipping and the port facilities which serve them. The ISPS Code is divided into two parts: Part A is mandatory and covers detailed security-related requirements for ships and port facilities, while Part B is nonmandatory and contains a series of recommendatory guidelines on how to meet these requirements. The focal point for port facilities is the ship–port interface, which encompasses the interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons and goods to and from the ship and the provision of port services. In order to comply with ISPS regulations, competent authorities must undertake port facility security assessments (PFSAs) and develop port facility security plans (PFSPs), and port facilities must appoint port facility security officers (PFSOs). Port facilities will also need to monitor and control access, monitor the activities of people and cargo, conduct searches and screening (dependent upon the requirements outlined in their PFSA and PFSP), and ensure that security communications are readily available. The PFSP details the mandatory security measures at various security levels. As an instrument aimed at risk mitigation towards international shipping and the port facilities which serve them, the ISPS Code also has the effect of reducing unauthorized third-party access to port infrastructure.

NOTES

12. The full list of 2020 amendments to the SOLAS regulations are available in an IMO press release, available online (accessed November 2020): https://www.imo.org/en/MediaCentre/PressBriefings/Pages/35-SOLAS-EIF-2020.aspx.

13. The IMO's Guidelines on Maritime Cyber Risk Management (Circular No. MSC-FAL.1/Circ.3, dated July 5, 2017) can be viewed online: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf.

14. The ILO/IMO Code of Practice on Security in Ports is available online at the ILO website: https://www.ilo.org/global/publications/ilo-bookstore/order-online/books/WCMS_PUBL_9221152863_EN/lang--en/index.htm.

144. ***The ISPS Code's primary objective is to reduce threats towards ships and port facilities.*** However, obvious indicators show the threat posed by cybersecurity is also addressed under this regulatory instrument, which has adopted an "all risks" approach to security. ISPS Code (Part A, 15.5.2) requires the PFSA to include the "identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures," which would include cybersecurity risks to port facilities, though the other elements of ISPS Code (Part A, 15.5)—including the identification and evaluation of important assets and infrastructure, identification, selection, and prioritization of countermeasures, and the identification of weaknesses, including human factors—would all involve cybersecurity risks, assets and vulnerabilities. Similarly, ISPS Code (Part A, 16.3.3), in regard to the PFSP, requires "procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship–port interface," which, again, would include cybersecurity. In addition, the ISPS Code (Part B, 15.3.5). requires that the PFSA identifies "radio and telecommunication systems, including computer systems and networks." Cybersecurity is, therefore, a threat that must be considered alongside the other risks to maritime security under the PFSA and PFSP for port facilities.

145. ***It is also important to note that cyberthreats might originate from ships and port facilities themselves, with negative implications for operations.*** An example is the malfunction or nonfunctioning of cargo-related IT systems either on the ship or shore side. As we have seen from incidents in the last few years, this can lead to a breakdown in port operations with broader implications for supply chains, and for national and international economies. Finally, a ship might itself pose a threat to the port facility, for example, it could be used as a base from which to launch an attack (ISPS Code, Part B, 1.4). Clearly, an important objective of the ISPS Code is to manage these broader cyber risks, leading to the conclusion that the role of the PFSO must encompass cybersecurity at the ship–port interface, rather than focus purely on more "traditional" physical threats. Indeed, this applies not just to cybersecurity at the ship–port interface, but more generally to cyber issues relevant for the wider well-being of maritime assets, infrastructure, and supply chain operations.

146. ***The International Safety Management (ISM) Code—Guidelines on Maritime Cyber Risk Management—is also helpful in this respect.*** The ISM Code, which was extended in 2017 with specific guidelines,[15] recognizes that cybertechnologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. The guidelines further acknowledge that the vulnerabilities created by accessing, interconnecting, or networking these systems can lead to cyber risks which should be addressed. In summing up the different areas for attention, the guidelines specifically mention cargo handling and management systems. The IMO's decision to extend the ISM Code with Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ. 3) acknowledges the functionality of a broader cyberhygiene to the security of shipping. As this basic approach closely mirrors the NIST Cyber Security Framework as outlined earlier in this section, and is also transferable to port facilities, a next step at the IMO level is welcomed to define how this should be operated in the context of the ISPS Code.

147. The ILO and IMO Code of Practice on Security in Ports ***extends the consideration of port security beyond the area of the port facility into the whole port and is much broader than the ship–port interface, which serves as the focus of the ISPS Code.*** The ILO/IMO Code recommends the development of a port security assessment (PSA) and port security plan (PSP) for the whole port area (in a similar way to the PFSA and PFSP for the port facility under the ISPS Code), and the appointment of a port security officer (PSO). Among other measures, the code recommends the "identification and evaluation of critical assets and infrastructure that it is important to protect," (7.1.1) and the "Identification of threats to assets and infrastructure in order to establish and prioritize security measures" (7.1.2). In addition the code also recommends that the PSP includes "details of security level 1 measures, both operational and physical, that will be in place," (8.1.3) and "details of the additional security measures that will allow the port to progress without delay to security level 2 and, when necessary, to security level 3" (8.1.4).

NOTE

15. The IMO's Guidelines on Maritime Cyber Risk Management (Circular No. MSC-FAL.1/Circ.3, dated July 5, 2017) can be viewed online: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf.

5.6 The Proposed Approach for Implementation

148. ***Port communities need to introduce a standardized approach methodology.*** After ensuring port facilities have addressed ISPS Code requirements and port communities have the infrastructure and mechanisms in place to share cyberphysical security information, port communities can begin planning investments around a standardized approach methodology. As port community members increasingly digitalize their operational environments, they must deploy integrated, digitally enabled cyberphysical security solutions that support ISPS Code compliance while also delivering appropriate, sustainable, and forward-looking security capabilities.

149. ***Ensuring cyberphysical security capabilities are suitable for specific maritime and port operating environments requires port community stakeholders to engage with subject matter experts in assessing current conditions.*** Successful engagement necessitates a phased approach, which links financial investments to key milestones—thus ensuring operational and financial alignment throughout the process—in designing the most appropriate, sustainable blend of integrated cyberphysical security capabilities, and ensuring deployed capabilities align with defined goals and performance objectives. To assist with investment planning, a potential approach is outlined below:

PHASE 1—DEVELOP AN ANALYTICAL FRAMEWORK

- **Task 1.1**—*Perform preliminary background investigation.* Collect and review relevant documents and other information regarding the port community and its members.

- **Task 1.2**—*Consult with port community leaders.* Interview key stakeholders to gather preliminary information and identify operational requirements and performance objectives. Relevant organizations may include port authority, customs, terminal operators, transportation entities (trucking, rail), pilots, law enforcement, and other first responders.

- **Task 1.3**—*Develop the project scope.* Discuss approach and review methodology and resource requirements, establish a communications plan, and examine current security issues and gather supplemental information. Develop a work plan and project schedule.

- **Task 1.4**—*Perform a feasibility study.* Develop a technical memorandum outlining the functions and operational requirements of the port community, its relevant integrated cyberphysical needs, and its security issues.

- **Task 1.5**—*Review findings with defined stakeholders.*

Ensuring cyberphysical security capabilities are suitable for specific maritime and port operating environments requires port community stakeholders to engage with subject matter experts in assessing current conditions.

PHASE 2—DEVELOP A SECURITY PROFILE

- **Task 2.1**—*Perform an assessment of the port community's (or member's) existing cyberphysical security capabilities.*

- **Task 2.2**—*Using inputs from Phase 1 and Task 2.1, develop a security profile.* The profile should define and characterize existing human capacity (including training), current processes and procedures, referenced standards, deployed technologies, integrated systems and platforms supporting security operations, information sharing mechanisms, guiding documentation (plans, strategies, and agreements), planned projects and initiatives, and current and planned budgets. Cyber, physical, and electronic security infrastructures and technologies, controls, interfaces, data workflows, and other relationships should be detailed, including any security operations center that may be in place or in the process of being implemented.

- **Task 2.3**—*Review findings with defined stakeholders.*

PHASE 3—DRAFT AND INTEGRATED SECURITY STRATEGY AND DEVELOP RECOMMENDATIONS

- **Task 3.1**—*Draft an integrated port community security strategy.* The strategy should support a common defense critical to the ongoing viability of port communities threatened by sophisticated threat actors. Coordinating such an effort requires the development of a coordinated security strategy that incorporates cyber, physical, electronic, and integrated data security elements, technology refresh requirements, and recommended policies and procedures under a unified governance framework.

- **Task 3.2**—***Develop recommendations for integrated cyberphysical capability specification options.*** Security capabilities comprise people (security staff, operational leaders), processes (alerts, notifications, information exchanges, and others), tools (security technologies such as CCTV systems, security information and event monitoring (SIEM) platforms, and environmental sensors such as aids to navigation), integration pathways (integrating real-time video and radar feeds and logging and monitoring of network activities), and budgets. Individually, such capabilities support day-to-day security operations, but when such resources are appropriately scaled, deployed, and integrated, port community stakeholders will derive far greater benefits via real-time or near-real-time actionable information.

- **Task 3.3**—*Develop security operations center options.* Rapid digitalization within port communities will require an integrated cyberphysical security strategy that considers a diverse group of stakeholders, operational needs, potential interoperability across a range of technology platforms and systems, and coordinated, secure information exchange. An integrated organizational structure will also require consideration to facilitate streamlined monitoring, analysis, communication, collaboration, and response processes structured to improve the port community's security posture, rationalize the utilization of human resources, and support the operational processes underscoring port-based commerce. A high-performing digital port security operation center should have the following technological capabilities:

> *As port community members increasingly digitalize their operational environments, they must deploy integrated, digitally enabled cyberphysical security solutions that support ISPS Code compliance while also delivering appropriate, sustainable, and forward-looking security capabilities*

- A scalable, integrated security management system;
- A security monitoring system with automated landside, waterside, and offshore (coastal regions, ports, anchorage areas, ship channels, and others);
- A centralized and virtual command and control capabilities;
- Integrated key technology platforms, such as CCTV, AIS, vessel traffic management information systems (VTMISs), radar, and drone surveillance platforms;
- Integrated data enrichment and processing capabilities (that is, utilization of advanced and/or predictive analytics and/or AI); and,
- Integrated security analysis and information sharing among stakeholders responsible for cyberphysical platforms.

- **Task 3.4**—*Review findings with defined stakeholders.*

150. ***Consider risk hedging through implementation of cyber insurance policies.*** Globally, insurers currently offer over US$1 billion in cyber insurance capacity and are increasingly designing new cyber policies with specialized coverage, increasingly robust cover, and higher limits. However, the lack of actuarial data remains a challenge. In response, insurers are more proactively engaging clients by seeking greater data on the extent to which clients have implemented and sustained cybersecurity capabilities across their organizations. This includes insurers requiring clients perform baseline assessments as a condition for binding and requiring recurring organizational cyber risk assessments as a condition of renewal. Insurers are also including within the policies a range of post-binding training and pre- or post-breach services, such as legal advisory, public relations assistance, forensic services, and call center support. These integrated service packages offer better options, pricing elasticity, and more comprehensive cyber risk management assistance to ports.

REFERENCES

Daffron, Jennifer. "Shen Attack Cyber Risk Scenario: Up to $110 Billion at Risk from Maritime Malware Attack." University of Cambridge Judge Business School, Centre for Risk Studies *Viewpoints* (blog), October 9, 2019. https://risk-studies-viewpoint.blog.jbs.cam.ac.uk/2019/10/30/shen-attack-cyber-risk-scenario-up-to-110-billion-at-risk-from-maritime-malware-attack/.

WEF (World Economic Forum). 2020. *The Global Risks Report 2020*. Geneva: WEF. https://www.weforum.org/reports/the-global-risks-report-2020.

Chapter 6: Implementing Digitization

6.1 Introduction

151. ***The COVID-19 crisis has exposed vulnerabilities in the trade supply chain logistics as worldwide disruptions in medical and food supplies impacted health, safety, and livelihoods of billions of people.*** Smooth functioning of maritime trade and supply chain logistics are integral to economic development as well as critical to food security and distribution of essential supplies, including life-saving vaccinations and medical equipment across the world. In a globalized world where maritime trade accounts for 90 percent of the world trade and global logistics market account for roughly 8 to 12 percent of global gross domestic product (GDP), the ports and supply chain logistics sector plays a highly sensitive and accountable role, necessitating leadership from the highest authorities to secure and efficiently manage the infrastructure services.

Smooth functioning of maritime trade and supply chain logistics are integral to economic development as well as critical to food security and distribution of essential supplies, including life-saving vaccinations and medical equipment across the world.

152. ***The available comparable indices indicate the impact of inefficiency on international trade.*** The World Bank Logistics Performance Index (LPI) and Doing Business Index (DBI) on trading across borders and the World Economic Forum's Global Competitiveness Index (GCI) 4.0 on efficiency on seaport services and border clearance indicate the extent to which inefficiencies at a nation's sea borders can impact international trade competitiveness. Technological innovations and digitalization provide opportunities to foster a more holistic approach and integrate the port ecosystem, thereby facilitating trusted partner collaborations between government agencies and the private sector and realizing significant efficiencies in port transactions.

153. ***However, the implementation of a successful digital program also requires high levels of political commitment.*** Strong policy reform toward change management, a clear communications plan and ideally a focal spokesman, a supporting legal framework, business processes optimization, automation, and reengineering between government agencies and private stakeholders stand out as immediate essential steps for nations to enhance the resilience and efficiency of supply chain logistics. This section identifies the institutional steps to manage the change processes to improve the resilience of the maritime logistic chain.

6.2 The Institutional Framework of a Digitalized Maritime Trade Platform

154. ***While the technology forms the backbone of a digital platform, the institutional framework and available human capital are crucial to ensuring its success.*** A successful digital platform needs to serve the interests of all its stakeholders and needs to be trusted. It also needs to be secure and resilient to the disruptions at process level as well as in the execution of nationwide infrastructure services. In addition, introducing and sustaining the platform requires adequate human capital, which calls for a trusted, neutral, and capable entity mandated to develop and operationalize an integrated system, in an open, transparent, and consultative manner.

A successful digital platform needs to serve the interests of all its stakeholders and needs to be trusted.

155. ***A high-level political commitment serves as the starting point to drive the change management process to digitalize the maritime, ports, clearance, and transport processes.*** Potential conflicts of interest and issues in a multipublic and multiprivate stakeholder environment in the short to medium term must be addressed, creating the need to introduce an appropriate, government-level legal basis. Institutionalizing the governance process at the government level, either by a ministerial cabinet decision or presidential decree, will layout the oversight mechanisms and decision-making responsibilities for the process.

156. ***The recommended approach is to establish a three-tiered framework to move the agenda forward.*** The recommendation suggests putting in place a governance framework designed to foster a holistic approach to developing efficiency and resilience of maritime trade and logistics, and structured at three levels—Level 1: an interministerial committee; Level 2: a steering committee; and Level 3: a business-level process committee. The roles and responsibilities of each are outlined in the following paragraphs.

157. ***Framework Level 1: The Interministerial Committee.*** The range of multisectoral, multidisciplinary responsibilities encompassed in an initiative of this type requires the establishment of an appropriate cabinet-level board forum, chaired by the prime minister or president's office. The committee will focus on the strategic coordination and the legal, regulatory, and policy issues. Table 6.1 outlines the proposed composition, scope of responsibility, and suggested frequency of meeting.

Table 6.1. The Interministerial Committee

Interministerial Committee	
Participants	• Minister of Transport • Minister of Shipping or Maritime Affairs • Minister of Finance and Economy • Minister of Foreign Trade and Industries • Minister of Commerce • Minister of Health • Minister of Agriculture • Minister of Immigration • Minister of Homeland Security • Minister of Information Technology and Digital Economy or State Secretary for Digital Affairs
Chair	Prime Minister or President's Office
Topics	• Champion the digital platform concept • Facilitate stakeholder cooperation • Supervise platform development • Drive policy reform and policy making • Review laws and regulations • Foster capacity building • Improve security • Promote the Fourth Industrial Revolution (4IR) • Drive innovation
Frequency	Quarterly

158. ***Framework Level 2: The Steering Committee.*** The Steering Committee should comprise the director generals of the public agencies and the presidents and secretary generals of private stakeholder organizations. The role of the committee is to lead the implantation of digital maritime trade and logistics roadmap, and play an instrumental part in the long term for the sustainability of the digital platform and systems. Critically, all key stakeholders must be included on the committee, with each allowed an equal voice. In strategic leadership roles, the committee chair and vice chairs will work to empower collaboration while leading the project and demonstrating their neutrality. The core public partners invited to the committee should include the port authority, maritime authority, customs authority, and foreign trade authority. Table 6.2 outlines the proposed composition, scope of responsibility, and suggested frequency of meeting.

Table 6.2. The Steering Committee

Steering Committee	
Participants	• Digital Ministry or State Secretary for Digital Affairs • Port Authority • Maritime Authority • Customs Authority • Foreign Trade Authority • Department of Immigration • Department of Health • Department of Agriculture • Department of Homeland Security • Terminal Operators Association • Shipping Lines and Agents Association • Freight Forwarder Association • Customs Brokers Association • Truckers Association • Rail Operators Association • Importers Association • Exporters Association • Insurance Association • Banking Association
Chair	Port Authority
Co-chair or Vice chair	Maritime Affairs and/or Customs and/or Foreign Trade
Topics	• Review project status report • Follow up on milestones • Follow up on deliverables • Discuss risk management • Discuss change management • Review the legal framework • Improve security • Follow up on action items • Follow up on issues • Discuss outstanding problems • Discuss proposed actions to be taken • Resolve deviations from schedule • Take corrective actions
Frequency	Monthly

159. ***Framework Level 3: The Business Process Committee.*** The third tier of the institutional architecture is the Business Process Committee. This committee should comprise representatives of all public agencies and private stakeholder organizations involved in the project. Each public agency and private stakeholder organization should nominate two persons, each recognized as a business process expert in his or her own organization. The committee will participate in the business process analysis, optimization, automation, reengineering, and rethinking of the digital road map. The committee will have a key role in the long term for the ongoing evolution and sustainability of digital business processes. Table 6.3 outlines the proposed composition, scope of responsibility, and suggested frequency of meeting.

Table 6.3. The Business Process Committee

Business Process Committee	
Participants	• Port Authority • Maritime Authority • Customs Authority • Foreign Trade Authority • Department of Immigration • Department of Health • Department of Agriculture • Department of Homeland Security • Terminal Operators Association • Shipping Lines and Agents Association • Freight Forwarder Association • Customs Brokers Association • Truckers Association • Rail Operators Association • Importers Association • Exporters Association • Insurance Association • Banking Association
Chair	Port Authority
Co-chair or Vice chair	Maritime Affairs and/or Customs and/or Foreign Trade

Business Process Committee	
Topics	• Review project status report • Follow up on milestones • Follow up on deliverables • Review as-is business process • Review to-be business process • Digitize all manual processes • Reengineer and reinvent all business processes as needed • Digitize all processes within port community • Introduce overtime and review new business procedures • Improve security • Imagine use cases for 4IR technologies • Foster best practices • Support in-change management activities related to implementation or introduction of new and reengineered processes within the port community • Implement standardization
Frequency	On request

160. ***Rather than establish a further series of committees, one option would be to use an existing modality.*** In December 2013, the World Trade Organisation (WTO) Trade Facilitation Agreement (TFA) was signed, and with it, WTO members committed themselves to create or maintain a national trade facilitation committee (NTFC). A recent report by the United Nation Conference on Trade and Development (UNCTAD 2020) underlined the need for countries to consider the NTFCs as permanent platforms that coordinate national trade efforts—not just to implement the WTO TFA, but also the trade facilitation reforms beyond it. However, challenges in the institutional setup have emerged in many countries, raising the need to further strengthen the NTFCs. The recent call to action by the International Association of Ports and Harbors (IAPH) and others on June 2, 2020, proposed the NTFCs could be an excellent instrument to help member states drive the change process in relation to the digitization of the maritime and logistics space. Setting up NTFCs to focus on the digitization effort would require a change in the mandate and their scope of action, but doing so will offer significant potential synergies.

161. ***The Government of Peru provides another example in response to the COVID-19 pandemic.*** The Government of Peru established on May 10, 2020, under Legislative Decree No. 1492, provisions to promote and ensure the reactivation, continuity, and efficiency of logistical operations of foreign trade, linked to the entry and exit of goods and means of transportation of cargo to or from the country. This includes the provision of freight and goods transport services linked to the foreign trade logistics chain, in all its forms as well as activities related to same in accordance with the provisions of the Ministry of Transport and Communications. The decree also includes provisions to procure the digitization of documents and processes of public and private entities, to optimize the time of operations, prevent and reduce the risk of contagion of personnel who provide services throughout the chain logistics, provide better health conditions, and finally, to guarantee the transparency in the costs of the services of the foreign trade logistics chain, which has been affected to a greater extent as a result of the health emergency national caused by COVID-19.

162. ***The Government of Peru recently affirmed the State has a duty to:*** (a) establish provisions to reactivate development of the logistics chain of foreign trade; (b) guarantee its continuity; (c) adopt provisions to promote the digitization of processes between public and private stakeholders that are part of the logistics chain; and (d) reduce the asymmetry of information between operators and promote the defense of the rights of consumers and users that participate in the logistics chain of foreign trade. Accordingly, on August 3, 2020, the Government of Peru published Supreme Decree No. 008-2020-MINCETUR, which regulates the Law of Strengthening of the Single Window for Foreign Trade (Law No. 30860). The decree also improves maritime single window (MSW) regulation and establishes a port community system under the aegis of the Ministry of Foreign Trade, including an interministerial committee.

6.3 Encouraging Innovation

163. ***In the context of accelerating digitalization in maritime trade and logistics, governments should also consider providing support for the development of digital incubators, accelerators, and early-stage funding programs.*** A new wave of incubators and accelerators in emerging and developing countries needs to be fostered to enable technology startups, supported by academic research, skills development and retraining, and outreach to attract talents and a new generation of digital maritime trade and logistics people in both the public and private sectors. Examples of such incubators and accelerators include DeltaX Ventures (Cartagena), founded by Sociedad Portuaria Regional de Cartagena; Pier71 (Singapore), founded by the Maritime Port Authority of Singapore and National University of Singapore; The Dock innovation hub (Haifa); Port XL (Rotterdam); and ZeBOX (Marseille). Government-supported incubators and accelerators should be designed to support the digital maritime trade and logistics entrepreneur on the path "from mind to market," that is, from the idea-stage of a business or product line, to the building of a prototype, to launching a new product, and finally to growing the business at home and abroad. Incubators should provide technical training, targeted business mentoring, and opportunities to network with the maritime trade and logistics ecosystem, investors, research institutes, and established firms. Accelerators should focus on helping already viable startups to enter a high-growth stage through intensive training and equity-based investment. In 2019, venture capital investment in maritime trade and logistics amounted to some US$8.74 billion in 532 companies.

164. ***A new era of governance to support digital maritime trade and logistics of the future will be needed beyond what exists today.*** New clusters of excellence will be required and will emerge, with some already forming at key hubs in developed countries mixing traditional port and maritime disciplines in new ways: PortXL in Rotterdam, The Dock in Israel, Pier71 in Singapore, and Delta X Ventures in Cartagena, are all substantive examples of new waves.

165. ***Many developing countries seek to improve the policy frameworks, technical programs, skills development programs, and financing initiatives that support entrepreneurship in the digital economy.*** The ultimate aim of these initiatives is to improve competitiveness, attract investment, create jobs, and grow markets. Young people, who are consistently the first to embrace new digital technologies, often seek employment in high-tech sectors and can be critical to developing a competitive, skilled workforce in an increasingly interconnected world. Furthermore, the digital economy contributes significantly to GDP in developed countries and is vital to spurring the overall innovation potential of a country in areas such as research and development (R&D), high-tech industry development, and technology patent activity. Time has come for emerging and developing countries to move forward.

6.4 How the World Bank Can Help

166. ***The World Bank Group (WBG) provides a unique repository of knowledge, technical assistance, and financial support for developing countries around the world.*** The WBG is not a bank in the commercial sense, but rather acts as a partner to assist countries in their journeys to reduce poverty and facilitate development. In the maritime sector, and the transport sector more generally, the WBG offers support to developing countries through policy advice, research, and analysis—drawing on the best global knowledge—along with targeted technical assistance to build capacity and development human capital in client countries. This analysis often underpins the case for public and/or private investment for priority projects and programs.

167. ***More specifically, in digitization of the maritime sector, the World Bank Group can mobilize financing for clients at different stages of their digital development path.*** The WBG can mobilize grant financing, subject to a successful application, from a range of potential sources—including, among other things, the Digital Development Partnership (DPP), the Public-Private Infrastructure Advisory Facility (PPIAF), and the Global Infrastructure Facility (GIF)—to facilitate upstream investigations to support clients in making informed choices about the how, the when, and the what of their evolution along the digital road. Subsequently, the WBG can facilitate, following a formal request and the necessary due diligence, financing in the form of concessional or semiconcessional finance, and possibly grants, to support agreed investments—either unilaterally or in partnership with private finance.

REFERENCE

UNCTAD (United Nations Conference on Trade and Development). 2020. National Trade Facilitation Committees as Coordinators of Trade Facilitation. Transport and Trade Facilitation, Series no. 14. https://unctad.org/en/PublicationsLibrary/dtltlb2020d1_en.pdf.

Appendixes

Appendix A: Port of Los Angeles—Port Community System Port Optimizer

BACKGROUND AND CONTEXT

168. ***The Port of Los Angeles, as one of the world's busiest seaports and leading gateway for international trade in North America, has ranked as the number one container port in the United States each year since 2000.*** In 2018, the port moved more cargo than in any time in its 111-year history—9.5 million twenty-foot equivalent units (TEUs)—the most cargo moved annually by any port in the Western Hemisphere. The port, also known as the Los Angeles Harbor Department, functions as a department within the City of Los Angeles and is governed by the Los Angeles Board of Harbor Commissioners, a panel appointed by the Mayor of Los Angeles. Although a city department, the port is not supported by city taxes. Operating as a landlord port with more than 300 leaseholders, the port instead generates its revenues from leasing and shipping service fees. The port's jurisdiction is limited to the Harbor District, which includes property in San Pedro, Wilmington, and Terminal Island. All port operations are managed by the Board of Harbor Commissioners in accordance with the Public Trust Doctrine to promote maritime, commerce, navigation, fisheries, and public access to the waterfront. As the busiest container port in North America, the port interacts daily with key supply chain stakeholders focused on promoting trade and to ensure trade volumes move through the port in a secure and efficient, and environmentally friendly manner.

169. ***Undoubtedly, the container shipping industry has been faced with difficult economic realities, further exacerbated since the onset of the 2008 recession.*** While the transition to ultra-large container vessels has yielded economies of scale, it has also led to new operational challenges for supply chain partners. Many shipping lines have entered into large shipping alliances, whereby up to six companies can share space on a ship—similar to the way commercial airlines share passenger space under codeshare agreements—causing greater complexity in cargo sorting and handling. Another challenge has been that supply chain information exists from numerous, separate sources—with supply chain partners often needing to access more than one dozen different websites for the information they need to manage their operations. Digitization facilitates this process,

as illustrated with the arrival of the 18,000 TEU container vessel, the CMA-CGM Benjamin Franklin on December 26, 2015. The port was honored to become the first North American port to receive an ultra-large container vessel. The Port was able to work with CMA-CGM and APM Terminals to use advance data to optimize the conveyance of the cargo and turn the ship around 13 hours in ahead of schedule. This experience has encouraged the port to further explore this approach by digitizing information sharing through a common portal.

PORT OPTIMIZER™ PILOT PROJECT AT THE PORT OF LOS ANGELES

170. Some of the primary challenges associated with a complex port operation such as that at the Port of Los Angeles include:

- Visibility to incoming ocean freight to enable unload planning, truck scheduling, and chassis allocations
- Vessels anchoring due to unavailability of berths
- Delays in the discharge of cargo
- Truck congestion due to inefficient planning and queuing processes
- Shortage of truck chassis for the containers
- Inefficient rail planning and utilization
- Limited labor forecasting

171. ***To assist in the resolution of the above challenges, the Port of Los Angeles set out to scope, manage, and execute a data and technology-based pilot project.*** The port wished to provide a single data, analytics, and technology solution that meet the multiple needs of its various constituents, facilitating better interoperability to result in increasing throughput and efficiencies within port operations.

172. ***On November 3, 2016, the City of Los Angeles Board of Harbor Commissioners approved an agreement to partner on the pilot project with General Electric (GE) Transportation to develop a first-of-its-kind, digital common user portal.*** GE Transportation was selected based on a public competitive request for proposal process performed by the Harbor Department. Through the pilot project, the port anticipated improved performance for its supply chain users over an historic baseline along multiple dimensions:

- **Operational and energy efficiency:** Use of the data would provide a line of sight to supply chain stakeholders so they can better allocate equipment and labor to handle cargo surges, thereby reducing cost and energy use.
- **Transparency:** Customs data would help provide supply chain users with visibility into the maritime supply chain, similar to what consumers expect from parcel service.

- **Reliability:** A line of sight into the supply chain would give users greater certainty and predictability, restoring the trust and reliability damaged during the congestion experienced in 2014 and 2015.

PRODUCT PRINCIPLES

The principles guiding the portal include the following:

- Fits within the existing supply chain ecosystem, creating a "system of systems," to enable interoperable supply chain visibility; the GE Transportation architecture and delivery mechanism is purposely flexible

- Explores, both openly and actively, potential technology partnerships across the maritime shipping and broader supply chain ecosystem

- Allows the client (in this example, the Port of Los Angeles) to retain ownership of their data and the ability to define data use, with GE Transportation acting as independent data steward and software provider

- Protects data privacy and does not share sensitive information housed within the portal, while maintaining open communication and transparency around data use

- Provides a highly elastic capacity to support easy, scalable, and both rapid and expected port growth

- Allows ample headroom to accommodate big data traffic

- Operates via a cloud-based, modular, and service-oriented system featuring a short release cadence, rapid production deployment, and experiment-oriented feedback and analytics

173. ***In collaboration with the pilot project participants, the GE Transportation portal, known as Port Optimizer, was developed to receive and provide supply chain information through a common user interface with secure channeled access by user type.*** Project participants include the United States Customs and Border Protection, the port's largest terminal operator (APM Terminal), the world's largest (Maersk) and second largest (MSC) shipping lines, along with a variety of beneficial cargo owners, trucking companies, and chassis providers.

174. ***The Port Optimizer portal went live with a limited launch on April 17, 2017, with a full launch for all pilot project participants on May 17, 2017.*** Since the portal went live, pilot participants have been able to view integrated supply chain data up to two weeks in advance of a ship's arrival at port, whereas previously data were available typically only three or four days in advance. Participant feedback has been very positive, who have expressed the desire to expand the pilot to include a greater portion of the port's supply chain.

175. ***The agreement between the Port of Los Angeles and GE Transportation (now known as Wabtec) was later expanded to further test the concept and benefits,*** adding scalability for single-window access to timely maritime supply chain information, and building upon the initial portal to add six more terminals and 15 more shipping lines.

176. ***The Board of Harbor Commissioners has taken several additional actions since the initial agreement, updating the scope of the Port Optimizer as illustrated in the following steps:***

- November 3, 2016 — Board approves pilot project
- April 17, 2017 — Port Information Portal (Port Optimizer) soft launch
- May 17, 2017 — Port Information Portal (Port Optimizer) live
- August 17, 2017 — Board approves expansion
- August 17, 2017 — Board approves revenue allocation agreement
- November 15, 2018* — Board approves name change to Wabtec
- March 21, 2019 — Board approves three-year extension, until November 2022
- October 8, 2019 — Board approves reallocation of funds and deliverables

*In February 2019, GE completed its spin-off and merger of GE Transportation with Wabtec Corporation.

177. ***To ensure the required data would flow into the Port Optimizer, the port rolled out a financial incentive program*** that rewards container shipping lines for growing their container businesses through the port faster than the total United States containerized Trans-Pacific import trade growth percentage. The port objective to handle all, and certainly increased container volumes, in the most efficient way possible, is possible with the Port Optimizer. As a condition to earn, this financial incentive shipping lines needed provide data into the Port Optimizer. The required data files are described in table A.1.

Table A.1. Port of Los Angeles: Digital Data Portal Electronic Transmission Schedule

Information	Frequency	Potential sources
Imports		Sources include, but are not limited to, the following:
Import manifest documentation (not including commodity or financial information)	Within 24 hours of origin departure; with all amendments or updates as generated	EDI 309—Customs manifest EDI 310—Freight receipt and invoice
Container stowage on incoming vessel	Within 24 hours of origin departure; with all amendments or updates as generated	BAPLIE—Origin and final EDI 324—Vessel stow plan
Marine terminal destination information	Within 24 hours of origin departure; with all amendments or updates as generated	IFTSAI
Container modality information (truck or specific railroad SCAC)	Within 24 hours of origin departure; with all amendments or updates as generated	EDI 404—Rail carrier shipment Information
Container final destination information	Within 24 hours of origin departure; with all amendments or updates as generated	Bill of lading
Container movement status updates	Within 15 minutes of movement event	EDI 315—Status details
Exports		
Export booking information (not including commodity or financial information)	Within 24 hours after booking accepted; with all amendments or updates as generated	EDI 301—Confirmation EDI 303—Booking cancellation
Export marine terminal information	Within 24 hours of origin departure; with all amendments or updates as generated	IFTSAI
Other		
Empty containers returned by marine terminal or container yard	Daily; with all amendments or updates as generated	Shipping line equipment management system
Marine terminal movements	Event-driven data shared as operations happen	EDI 322—Container discharge, load, ramp, deramp, gate in, gate out
Terminal operating system API feeds	Event-driven data shared as operations happen	Marine terminal events, status and updates (yard location, last free day, holds)

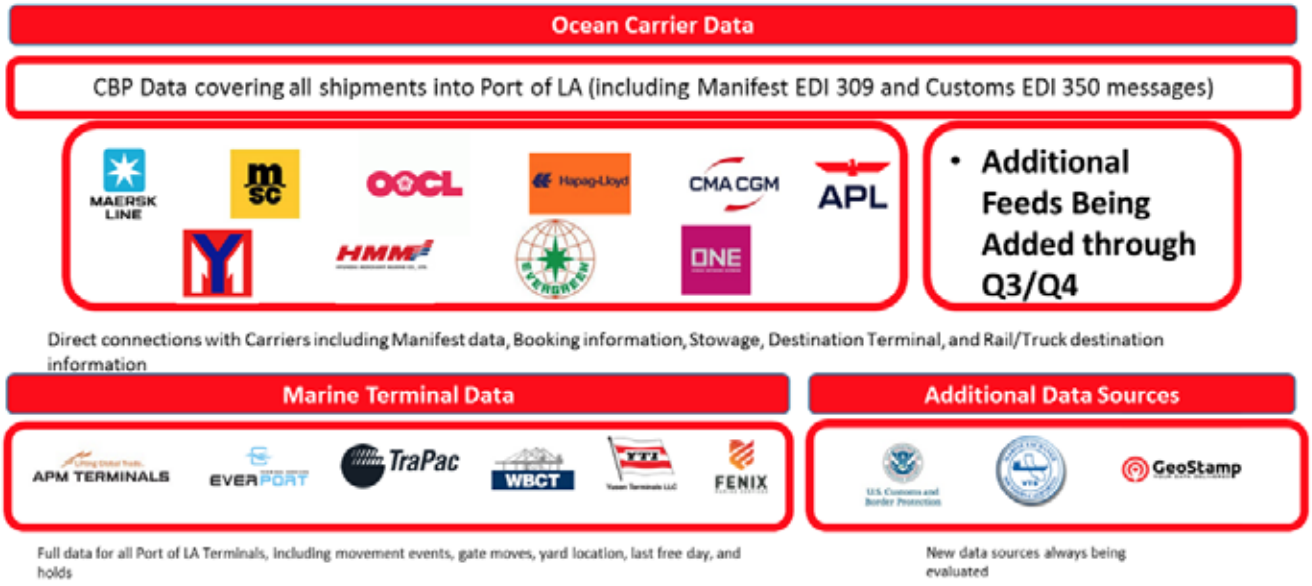
Information	Frequency	Potential sources
Item 255—Imports		
Import manifest documentation (not including commodity or financial information)	Within 24 hours of origin departure; with all amendments or updates as generated	EDI 309—Customs manifest EDI 310—Freight receipt and invoice
Container stowage on incoming vessel	Within 24 hours of origin departure; with all amendments or updates as generated	BAPLIE—Origin and final EDI 324—Vessel stow plan
Marine terminal destination information	Within 24 hours of origin departure; with all amendments or updates as generated	IFTSAI
Container modality information (truck or specific railroad SCAC)	Within 24 hours of origin departure; with all amendments or updates as generated	EDI 404—Rail carrier shipment information
Container final destination information	Within 24 hours of origin departure; with all amendments or updates as generated	Bill of lading

Note: API = application programming interface; BAPLIE = bayplan/stowage plan occupied and empty locations message; EDI = electronic data interchange; IFTSAI = international forwarding and transport schedule and availability information message; SCAC = standard carrier alpha code.

178. ***In addition, the port tariff was amended requiring marine terminal operators to provide additional data elements into Port Optimizer (figure A.1).*** The effect of those two actions accelerated participation of container shipping lines and marine terminal operators in Port Optimizer.

179. ***All seven of the port's container terminals provide data as well as nine of the top ten major global container shipping lines.*** The COVID-19 pandemic has required the port to reinvent itself very quickly, with the first order of business to protect essential workers, followed by speeding critical supplies through the supply chain. To that effect, Los Angeles Mayor Eric Garcetti named Gene Seroka as the chief logistics officer for the City of Los Angeles, which he holds concurrently with his job as executive director of the Port of Los. As chief logistics officer, Mr. Seroka's goal is to ensure frontline medical workers get the required personal protective equipment (PPE), and to look for alternative PPE manufacturers to fill the need. This work is underpinned by digital technology referred to the "Medical Optimizer," a bolt-on feature of the Port Optimizer. The Medical Optimizer has allowed area hospitals the ability to track their inbound medical supply shipments through the Port of Los Angeles and the Los Angeles World Airports, expediting them to destinations as they arrive. More information is available online: https://www.lovla.org.

Figure A.1. Port Community System Data Sources



Source: Port of Los Angeles

Appendix B: Port of Shanghai—Creating a Port Community System and a Smart Port

OVERVIEW OF SHANGHAI PORT

181. ***Shanghai Port is a container port serving mostly import and export cargos.*** Its annual container throughput grew from 1 million twenty-foot equivalent units (TEUs) in 1994 to more than 43 million TEU in 2019, making Shanghai Port the world's largest container port for ten consecutive years. As of August 2020, the average daily operating statistics of Shanghai Port are listed as follows:

- **130,000** TEU throughput
- **200,000** containers handled
- **1,500** transloading vehicle trips
- **47.5** mainline vessel calls (100 at peak)
- **115.6** feeder vessel calls (400 at peak)
- **50,000** container trucks (peak hour 3,000 trucks)

182. ***Shanghai Port's public terminals are operated by Shanghai International Port Group (SIPG), which is a conglomerate established in 2003 after the restructuring of the former Shanghai Port Authority.*** In 2005, SIPG was restructured to become a share-holding corporation, which was listed in the Shanghai Stock Exchange in 2006, thus becoming the first port share-holding corporation listed in China. At present, SIPG is the largest listed port company in mainland China and one of the largest port companies in the world. It is primarily engaged in port-related business in four areas: container, bulk cargo, port logistics, and port services.

183. ***Early on, Shanghai Port recognized the critical role an information and communications technology (ICT) system could play in increasing its competitiveness.*** Import and export maritime shipping involves many stakeholders, lengthy processes, multiple intermediate steps, high-cost intermediate services, and a low degree of information sharing. Additionally, the relationships and interactions between the stakeholders is complex. A well-developed ICT system will facilitate information sharing among the many stakeholders, reduce redundancy in processes and documentation, remove operation bottlenecks,

and improve efficiency. As such, Shanghai Port established Shanghai Harbor e-Logistics Software Co., Ltd. (Shanghai Harbor e-Logistics) in 2001 to develop port ICT systems with a mission to become a top provider of smart port solutions. After SIPG was established, Shanghai Harbor e-Logistics became a subsidiary of SIPG.

DEVELOPMENT OF A PORT COMMUNITY SYSTEM

184. ***Shanghai Port's smart port development comprises four components: terminal operation management, cross-terminal operation management, logistics service, and financing and other auxiliary services.*** The smart port development focuses on connecting terminals, shipping companies, shipping agencies, freight forwarders, trucking companies, warehouses, storage yards, regulators, and law enforcement agencies to create an open and community-based information platform, in essence a port community system (PCS). Shanghai Port PCS expands beyond the traditional business model that focuses on terminal operation to integrate the whole logistic value chain and create new business opportunities. It makes doing business with Shanghai Port easier for customers because it simplifies procedures, expedites processes, reduces cost, and improves efficiency. Figure B.1 illustrates the key stakeholders of Shanghai Port PCS, while figure B.2 illustrates components of Shanghai Port blockchain-based PCS.

Figure B.1. Port of Shanghai: Port Community System Stakeholders

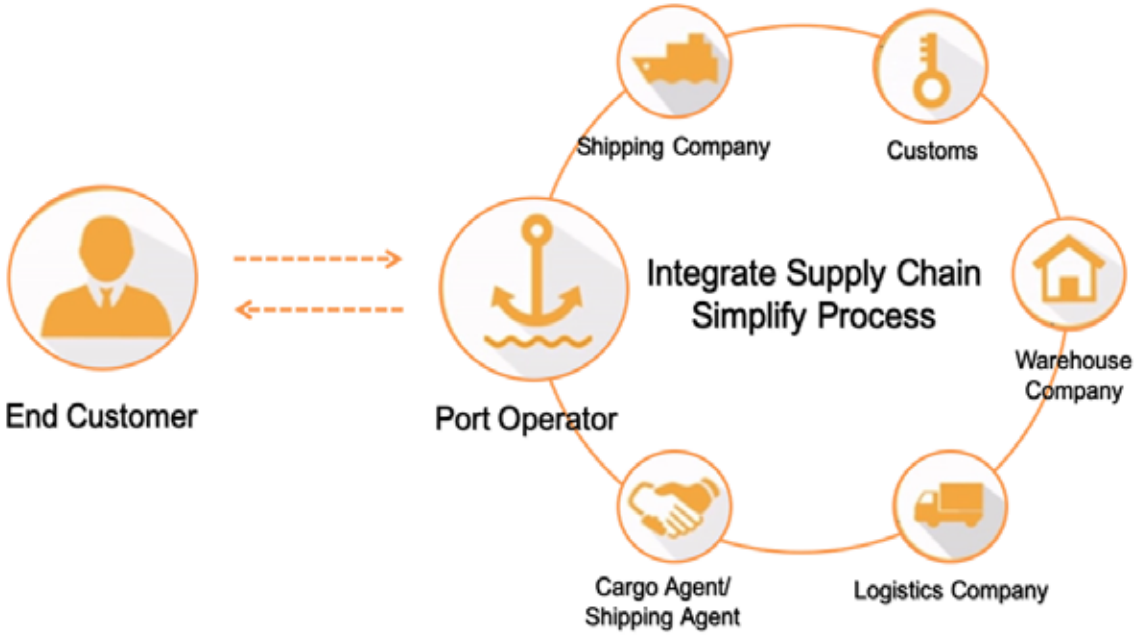
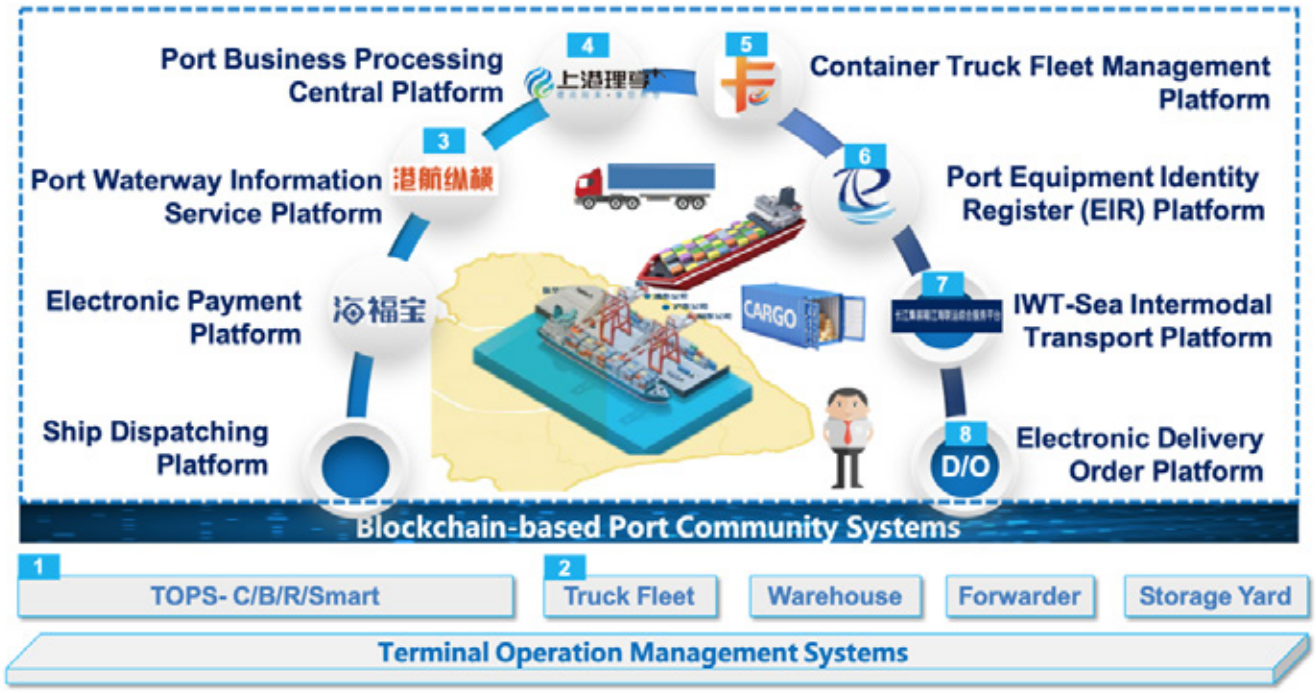


Figure B.2. Port of Shanghai Port Community System



185. ***A terminal operation system (TOS) processes essential daily workflow, including planning, dispatching, monitoring, and control, and plays a critical role in ensuring throughput and customer service quality of an individual terminal, which is on the critical path of the global logistics chain.*** Shanghai Port, as a gateway of international trade serving the vast Yangtze River Delta hinterland, manages multiple sea terminals and inland waterway transport (IWT) terminals, each specialized in container, bulk, and roll-on/roll-off businesses. To optimize operations of the many terminals within Shanghai Port, such as transloading from sea terminal to IWT terminal, Shanghai Harbor e-Logistics developed a port territory-wide cross-terminal operation management system.

186. ***In April 2012, Shanghai Port operationalized its first cross-terminal operation management system.*** Shanghai's terminal operation management system, or TOPS, as shown in figure A2.2 (1- terminal Operating System -Container terminal, Bulk terminal, Ro-Ro Terminal [TOPS-C/B/R/Smart]), coordinates the dispatching, operating, and monitoring between Waigaoqiao terminal and Yangshan terminal. As of 2020, the cross-terminal operation management systems dispatch 130,000 TEU and 250 ships daily.

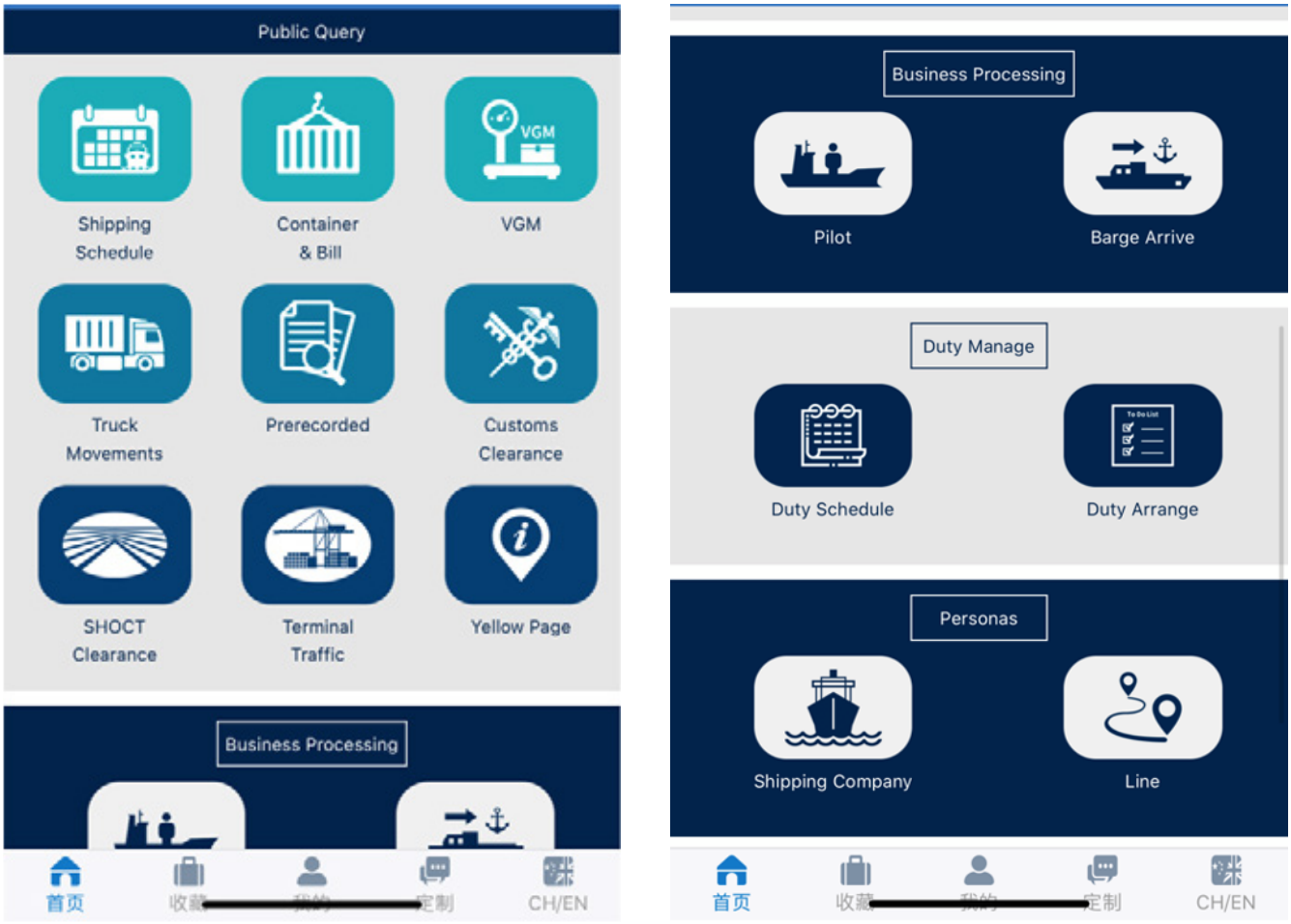
187. ***Learning from the business model of Uber—the car hailing application, In March 2013, Shanghai Port deployed a cross-terminal container trucks transloading platform.*** The platform supports two-way transloading operations of container trucks across multiple container terminals, processing more than 2,000 TEU every 24 hours. The heavy loading-in and heavy loading-out ratio of internal container trucks with one-side container trailing has increased from zero percent to more than 80 percent, while empty loading ratio reduced from 50 percent to 26.47 percent. With the same level of service, diesel consumption within the entire port area reduced by 4,000 tons, representing a 43.75 percent reduction of the port's total diesel consumption.

COORDINATED MARITIME LOGISTICS, AND INCLUSIVE FINANCING AND FACILITATION

188. ***In December 2014, Shanghai Harbor e-Logistics developed an information platform, Ganghang Zongheng, to standardize and integrate operation information of Shanghai Port and more than 20 river ports along the Yangtze River***, thus enabling one-stop, global, real-time tracking of ships, containers, cargos—including vessel name, voyage number, operation node, and location of containers and cargos. Figure B.3 illustrates the Ganghang Zongheng customer interface. As of July 2020, the platform has more than 180,000 registered customers, more than 1 million daily queries, and 300 million queries a year.

189. ***In July 2015, the online central port business platform at Shanghai Port commenced operation***, allowing forwarders to process import business and make electronic payments for maritime shipping and port charges of all Shanghai Port container terminals. As of August 2019, import businesses are now almost all processed online, reducing required business processing personnel by 40 percent, labor costs by 60 percent, and carbon emissions by 90 percent.

Figure B.3. Ganghang Zongheng User Interface



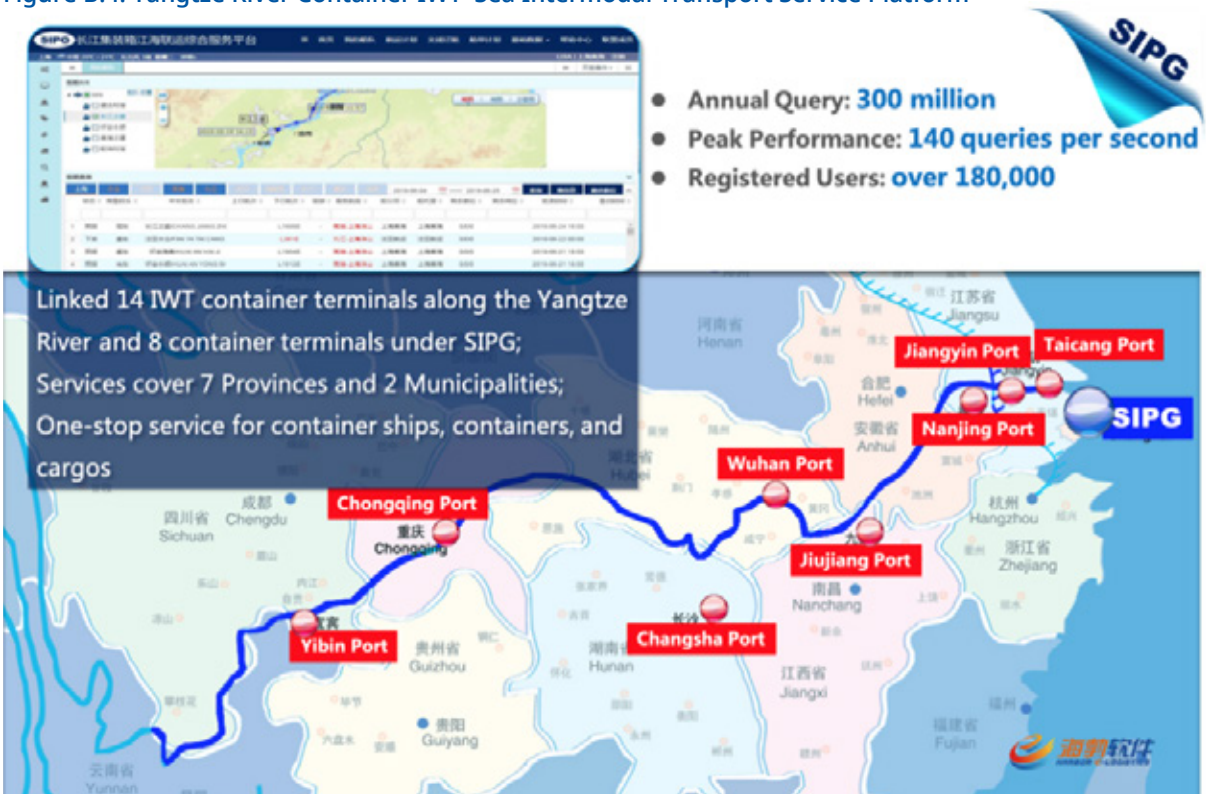
190. ***In October 2016, Shanghai Port launched a mobile service platform, E-Truck Zongheng, allowing private container trucks to make appointments for port entry on the mobile platform.*** This platform coordinates terminals, storage yards, truck fleets, machineries, and other services to improve efficiency of container transport. With more than 90,000 registered users covering almost all active container trucking operations in Shanghai, the platform has reduced truck fuel consumption and optimized resource utilization.

191. ***In July 2018, Shanghai Port launched the Electronic Equipment Identity Register (EIR) platform.*** The EIR standardizes and digitizes the traditional equipment paper receipts previously in use for forty years. In the same year, EIR paperless processing was operationalized for trucks entering or exiting terminals for container pick-up or drop-off. The EIR platform has saved an estimated RMB 400 million (in renminbi, equal to US$57 million) per year, after eliminating the production cost of 15 million paper documents valued at RMB28 (US$4)

each. Looking at imports, the wait time from cargo arrival to cargo pickup has been reduced from 4.5 days to one day, since companies no longer need to process the release of container cargo at a physical window. Instead, the EIR allows the cargo releasing companies, truck fleet, and container truck drivers to exchange the required documents electronically around the clock.

192. ***In 2018, entrusted by the National Development and Reform Commission (NDRC, the national planning agency), Shanghai Harbor e-Logistics developed and promoted an integrated service platform for the Yangtze River container IWT-Sea intermodal transport service.*** The platform, as illustrated in figure B.4, serves individual ports along the Yangtze River—scattered in location and fragmented in service offerings—along with feeder line operators, shipping agencies, freight forwarders, and other service providers to better share information and resources, and improve business. The platform will support the Yangtze River Economic Belt Shipping Alliance, jointly initiated by nine port groups, including SIPG, Nanjing Port Group and Jiujiang Port Group, and five shipping companies, including China Yangtze Shipping Group Company, Ltd., and Yangtze Port Logistics Company, Ltd., to further develop shipping potential of the Yangtze River Economic Belt.

Figure B.4. Yangtze River Container IWT–Sea Intermodal Transport Service Platform



193. ***In January 2019, Shanghai Port launched the Electronic Delivery Order Platform, based on blockchain technology*** and integrated with EIR, Shanghai Port's unified business processing center platform; the E-Truck Zongheng container truck fleet management platform; and the Ganghang Zongheng port and waterway information service core platform to further improve doing business with Shanghai Port. To date, the bill of lading issuance rate exceeds 99 percent. More than 7,000 bill of lading orders and 17,000 TEU container transfer have been completed. In November 2019, Shanghai Port completed the first paperless transaction of packing list, EIR, and delivery order.

COORDINATION WITH THE SHANGHAI INTERNATIONAL TRADE SINGLE WINDOW

194. ***The Shanghai International Trade Single Window aims to achieve "one declaration, global customs clearance" and become a key node of the global trade network.*** The single window for China (Shanghai) international trade has completed version 3.0, with data from April 2019 showing that 100 percent of goods declaration and export tax rebate services in Shanghai Port are now processed through the single window. The single window features 15 functional modules, including goods declaration and transport mode declaration. Connected with 22 government agencies and serves 280,000 companies, the single window has reduced the time needed for cargo declaration from one day to 0.5 hours, and ship declaration from two days to two hours.

PCS SUPPORT IN RESPONSE TO CHALLENGES STEMMING FROM COVID-19

195. ***During the COVID-19 outbreak, Shanghai Port PCS was able to provide contact-free and zero-delay services to customers.*** Taking the delivery of goods as an example, customer verification, agency operation, payment, transport arrangement, and other related work can now be completed online. It not only saves time and cost, but also ensures health and safety. As a full-service marine logistics provider, Shanghai Port continues to explore "port for city prosperity and city for port development," with the vision of becoming a globally outstanding terminal operator and port logistics service provider. Shanghai Port PCS development principles are as follows:

- **Change the development model from individual to synergy.** The port logistics information network should be built to realize the information interconnection of the key stakeholders in the port supply chain. The traditional independent development model based on terminal operations should be changed to an integrated model based on the logistics chain, cross-region, and cross-port operation.

- **Change the service model from passive to active.** The establishment of a unified external service window is necessary to realize the port business one-stop processing and comprehensive information query, and to change from the traditional passive "to give what customers ask" to more active service mode.

- **Change the management model from fragmentation to systematization.** The visualized tracking of the entire cargo transport process changes the relatively independent resource elements and management process to the digital and intelligent management model.

PHOTO CREDITS

Cover Page, page 133: Shutterstock
Page 7: Rob Beechey, World Bank
Page 10, 13: Unsplash Timelab Pro
Page 21: MIT Panama
Page 27: Dominic Sansoni, World Bank
Page 34, 41: Stock Image
Page 35, 36, 37: Rombit Port of Antwerp
Page 38: Port of Antwerp, Belgium
Page 39: Henitsoa Rafalia, World Bank
Page 40: Port of Acu
Page 42: Rob Beechey, World Bank
Page 49, 51: IAPH
Page 53: E Van Caeneghem
Page 67, 68: Shutterstock
Page 71: Mauro Tema, World Bank
Page 77: Port of Antwerp, Belgium
Page 81, 82: Stock Image
Page 87: Unsplash Markus Spiske
Page 88: Stock Image
Page 91: Mauro Tema, World Bank
Page 97: Port of Los Angeles
Page 102: Mauro Tema, World Bank
Page 106: Stock Image
Page 115: Shutterstock
Page 117: Rob Beechey, World Bank
Page 124: Dominic Sansoni, World Bank


WORLD BANK GROUP


IAPH
International Association
of Ports and Harbors


WPSP
WORLD PORTS SUSTAINABILITY PROGRAM