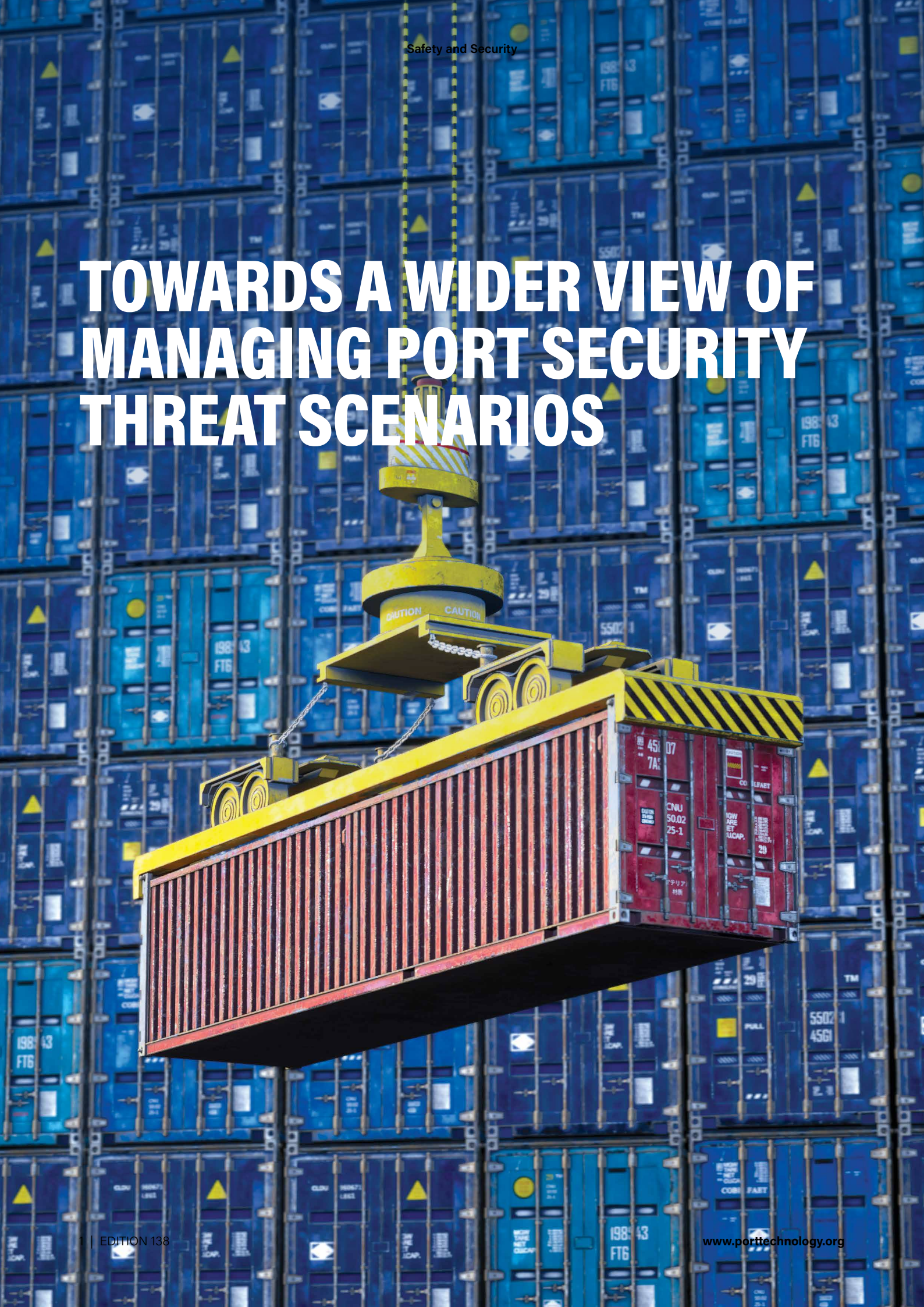
TOWARDS A WIDER VIEW OF MANAGING PORT SECURITY THREAT SCENARIOS



Richard Oloruntoba, Associate Professor in Logistics and Supply Chain Management, Curtin Business School, Curtin University, Perth, Western Australia

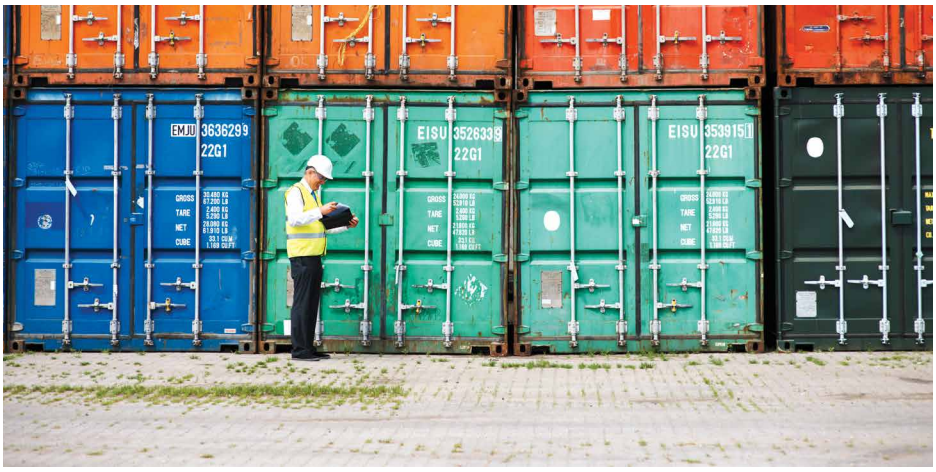
INTRODUCTION

Since the terrorist events of 11 September 2001, the attention of port managers and others has shifted to matters of port security, whether sea or air. Indeed, security and safety assurance across maritime trading systems has become a critical and ongoing factor for international business managers and international trade. Port security is a small part of broader maritime security. Port security has to do with treaties, defence and law enforcement, as well as counter-terrorism activities within the port and extending to the maritime domain. Since 9/11, port security measures have focused on the protection of (a) seaports (b) cargoes moving through the ports, and (c) personnel moving through or working in ports. Port security risk management focuses on the physical security of the port and its perimeters, its cargoes, the ships departing or arriving within port waters and the harbour, and any risks to the continuity of port operations as well as the safety of port data. Additionally, the port is connected to a much larger supply chain with various risks along the chain that can and do affect port security.

The International Maritime Organization (IMO) has a security framework of rules that govern port security globally. For instance, the 2002 International Ship and Port Facility Security Code (ISPF Code), and the Safety of Life at Sea (SOLAS) Convention address ship security and requirements for compliance with the ISPS Code, including ship identification, security planning, and alert systems that have been mandated, Similarly, the World Customs Organization (WCO) and the International Maritime Bureau (IMB) have supported processes that enhance broader regulatory coverage of safety and security within the world trading system.

In addition to IMO port security rules, the United States unilaterally introduced its own Container Security Initiative (CSI) and the Customs Trade Partnership Against Terrorism (CTPAT). The main aim of all these initiatives is to reduce the likelihood of maritime-vectored terrorism in port premises and other human-induced port security breaches. Although some analysts have argued against the implementation of port security governance measures based on

"SECURITY AND SAFETY ASSURANCE ACROSS MARITIME TRADING SYSTEMS HAS BECOME A CRITICAL AND ONGOING FACTOR FOR INTERNATIONAL BUSINESS MANAGERS AND INTERNATIONAL TRADE."



"HALF OF ALL MARITIME INCIDENTS IN 2022 OCCURRED IN PORTS AND TERMINALS."

its prohibitive costs, threats to competitiveness, and ineffectiveness, it appears there has been growing consensus internationally, in recent times, that security governance measures are a necessity because of new and evolving threats and risks. Examples of such new threats and risks include malicious port operations breakdown, illegal entry of contraband material including humans, fraud, geopolitical tensions, military conflict, cyber and ransomware attacks, and technological failures amongst others. Most recently, the handling and storage of lithium batteries in and out of electric vehicles is of increasing safety concern to ports. Half of all maritime incidents in 2022 occurred in ports and terminals according to Seatrade Global Port Report 2023, and when safety and security incidents disrupt operations, they can set off a cascade effect across the supply chain. In essence, economic and trading boundaries have become 'security' and 'safety' boundaries. Hence, this article argues that the expected reliability and assurance of port security and maritime trade will not arise from mere adoption, compliance, and implementation of port security governance frameworks alone. The article suggests that effective security outcomes will only result from properly integrating underlying risks, and safety and security concepts into existing managerial practice, and making sure they are systemic and sustainable.

The rest of the article is structured as follows: first, the article discusses several well-recognised risk factors within the international maritime trading system; second, it highlights the value of ports undertaking scenario and vulnerability analysis for on and offshore aspects of maritime commerce for preparedness. The article concludes by identifying a couple of urgent issues relevant to port security policy and management within the port and maritime supply chains.

COMMON RISKS: OLD AND NEW

Increasing trade volumes and sub-standard vessels

The United Nations Conference on Trade and Development (UNCTAD) in their 2022 report highlighted that in 2022 globally, 4.6 million port calls were recorded, and growing. The increased flows of trade, port calls, and increasing size of ships are sources of risk to safety and security in ports. The enormous trade volumes passing through ports have prompted them to pursue efficiency through automation and advanced information and communication technologies, which could also be a solution to personnel safety. Also, there are unknown risks arising from sub-standard vessels arriving in port, which could result in safety-related incidents that could disrupt port operations. A recent Seatrade article reported that vessel-related safety incidents in ports in 2022 alone resulted in 175 fatalities, 114 missing persons and 76 serious injuries, globally. Furthermore, 1,955 vessels were detained by Port State Control for 10,445 days for serious non-compliance with international safety regulations. Safety-related incidents could occur anywhere within the remit of the port authority such as while transiting channels, at berth, while using facilities, or while at anchorage. Hence, ports and harbourmasters need to pay close attention to managing this concern.

The complexity of modern port operations

A different perspective on risk factors for ports is the recognition of the complexity of modern port operations and the challenges of effectively implementing safety and security coverage over them. The Ammonium Nitrate explosion at the Port of Beirut on 4 August 2020 caused 204 deaths, more than 7,000 injuries, and a loss exceeding $ 15 billion, with 300,000 people left homeless. Tonnes of Ammonium Nitrate (AN) confiscated by Lebanese authorities from the abandoned vessel 'Rhosus' were stored in a warehouse within the port for almost six years without good safety management. The explosion was preceded by a fire resulting from welding work to repair the warehouse door.

With enormous volumes of international maritime cargo movements, and up to 90 per cent of world cargo movements by tonnage occurring in shipping containers, the size and complexity of ensuring safety and security staggers the imagination. Of this

trade, less than 10 per cent is subjected to physical inspection after arrival at a destination. The issue of complexity parallels a suite of practices that further add layers of risks and grounds for concern about safety and security matters generally. Security and safety risks often emerge from the interaction of factors such as:

- **The cargo and nature of cargo** – i.e. hazardous cargoes of a conventional, explosive, flammable, nuclear, chemical, or biological nature, and using cargo containers to smuggle people and/or weapons;
- **The vessel** – using the vessel as a tool or weapon or a means to launch an attack such as sinking a vessel in the channel or at berth to disrupt infrastructure;
- **The people** – using fraudulent identity in support of criminal and/or terrorist activities;
- **The lack of transparency in ship registration and ownership** – i.e., the absence of clear registration details, and anonymity of vessel ownership is a standard shipping industry practice that can enable a cloak of anonymity.

Cybersecurity risks

Seaports often deploy and are reliant on advanced information and communication systems that are in turn reliant on automated satellite-based internet systems. These information systems are vulnerable to being hacked for ransom, or hacked to disrupt port operations and in turn, global supply chains. Hacking of vessel-based systems may also be used to illegally track, mislead or divert vessels for hijack.

US seaports alone handle more than $5.4 trillion in goods every year, making US ports a unique target for cybercriminals. The same is true for major hub ports like Singapore, Shanghai, Hong Kong, Rotterdam, Busan, Ningbo-Zhoushan and others. Moreover, more than 500 cyberattacks were reported to have occurred in the global maritime industry in 2020, according to the U.S. Coast Guard. These cyberattacks were targeted at conventional information technology systems such as networks, data and proprietary information. The attacks include malware, ransomware, spear phishing and credential harvesting. Other attacks may target operational technology (OT) systems such as gantries, cranes, lifts and conveyance systems that lift on and lift-off cargoes on and off vessels, to paralyse port operations. Attacks may also aim at paralysis of port gates and truck loading and offloading operations.

"SCENARIO DEVELOPMENT AND ANALYSIS PROVIDE A MEANS FOR DECISION-MAKERS TO ANTICIPATE POSSIBLE INCIDENTS AND SCENARIOS AND STRATEGIES TO MITIGATE LIKELY ADVERSE IMPACTS."

Liquefied natural gas risks

The increasing import and export trade in liquefied natural gas is an emerging safety risk in an increasing number of offshore and onshore ports, globally. Port gas infrastructure networks are often extensive with storage, liquefaction, regasification and distribution networks in terminals. Liquefied natural gas (LNG) comprises explosive methane, butane, propane and ethane. Hence, many port terminals with LNG facilities are concerned about highly flammable LNG cargoes which is a safety and security risk to staff members, and adjoining communities and populations. The whole chain of supplies of LNG and storage must be securely and safely managed with sustained risk management processes put in place beyond the port itself.

SCENARIO AND VULNERABILITY ANALYSIS MAY BE A WAY FORWARD

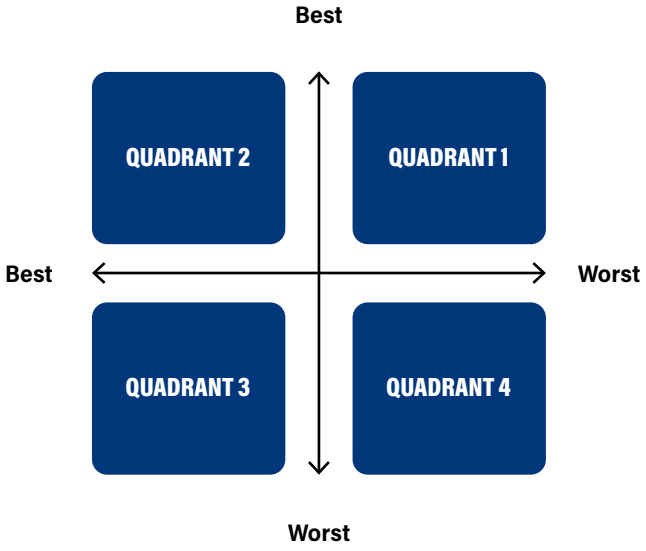
Scenario development and analysis provide a means for decision-makers to anticipate possible incidents and scenarios and strategies to mitigate likely adverse impacts. In the scenario methodology, each scenario considers how the future might eventuate by analysing past, current and possible situations or scenarios, and creating informed assumptions.

The scenario development process entails identifying past and current environmental pointers and constructing expressive images based on possible, and plausible, future happenings in the port. Plausible scenarios could be developed based on a desk review of relevant literature such as published case studies and exemplars, publicly known historical incidents and accidents, security analysts' reports, relevant media analysis and commentaries and similar other sources relevant to security and safety issues in the context of ports and their connected hinterlands and maritime supply chains. Such analysis of literature can be supplemented with a scenario thinking workshop informed by reconstructed historical accounts of past security and safety incidents, geopolitical debates, and accounts of knowledgeable individuals. The scenarios with the most significant uncertainties would then be selected for consideration, identification of possible outcomes, and development of managerial and policy recommendations. The process involves constructing expressive images based on possible, and plausible, future happenings and assessing their impact on operations, finances and supply chains. The next stage in scenario thinking is the generation of an impact and certainty matrix. This matrix reveals the impact and certainty/likelihood of each possible outcome of the studied event. Participants in a scenario thinking workshop would be asked to consider the current and future impacts of various dimensions of the scenarios, their level of certainty, and plausible scenario outcomes.

A consideration of the positive and negative aspects of the key issues is the focus of the scoping and building of scenarios. The threat dimensions of the scenarios may be dissected into four quadrants to provide the basis for scenario building on a best-worst continuum on each of the X and Y axes. The quadrants represent a set of conditions to define four possible combinations e.g., best-best, best-worst, worst-best and worst-worst conditions in which the impacts of a particular type of port safety and security risk might unfold. The worst-worst scenario is quadrant 4 with maximum adverse impacts and the best-best scenario is quadrant 2 with minimal adverse impact from the identified port security and safety risk.

Prioritisation of the worst-worst risks for management based on severity and certainty of impact is key to managing the most important port safety and security risks, and this would be different from one port to another. Some risks would be relatively manageable, whilst others would be more challenging to manage. Cyberattacks for example would likely exert an enormous adverse

"PORT SECURITY IS CRITICAL TO ECONOMIC SECURITY AS SEEN FROM VESSEL VOYAGES THAT HAVE THEIR DEPARTURE, ARRIVAL OR DESTINATION POINTS IN A PORT."



impact on port IT systems, as such disruptions and safety concerns are far more likely to occur, given the rapid pace of port automation and self-directed navigation of vessels. Maersk IT and communications systems were paralysed by the NotPetya worm for two weeks in 2017, affecting 800 vessels and 76 ports across the world, and costing the company almost $300 million.

Wider vulnerability analysis

Vulnerability analysis considers how vulnerable a port and its hinterland and overseas shipping connections are to the previously identified safety and security risks and the worst-worst scenario. Vulnerability analysis is conducted in four main steps. In the first step, AIS transponder data of vessels may be used to explore port-to-port seaborne trade of groups of commodities with other countries in the region and globally, e.g. iron ore, crude oil, or containers. The AIS data helps to identify ports involved in particular commodity seaborne trades within the shipping network. In the second step, we can gain insights into the role of the port being analysed for vulnerability within the network as regards the specific commodity group under analysis by varying a range of measures at the network and node levels.

In the third step, import chains of specified commodities are mapped to gain further insights into the vulnerability of a particular port. This mapping supports the fourth step, which includes a scenario analysis of port safety and security risks and broader maritime security threats such as those emanating from international shipping, and allied vulnerabilities. For example, current military challenges from Houthis in South Yemen in the Red Sea have had a significant adverse impact on port arrivals in ports in Sudan, Eritrea, Djibouti and Somaliland region, and on vessel traffic in the Suez Canal as many vessels re-route via the Cape of Good Hope in South Africa.

Hence, the concept of port security and operational disruption risks is broader than the physical security of port premises, infrastructure, approaches and channels. Port security is critical to economic security as seen from vessel voyages that have their departure, arrival or destination points in a port. This is because the port is a node in the network of vessel sailings for a specific commodity. For example, interruptions to vessels transporting crude oil from the Middle East/Persian Gulf to Japan are expected to affect the operations of receiving ports and refineries in Japan.

SUMMARY AND ISSUES OF PORT SECURITY POLICY AND MANAGEMENT

The article has discussed the concept of port safety and security and highlighted that port security extends to the broader supply chain with various safety and security risks along the chain, which affects port security, and thus requires management. The article discusses many well-known safety and security risk factors for ports within the international maritime trading system and suggests scenario and vulnerability analysis methods for managing risk and enhancing preparedness through mapping vulnerability within ports and across supply networks. Scenario development and vulnerability analysis provide a means for decision-makers to anticipate broader port-centric risks and mitigate likely impacts.

The article also suggests that the complexity of interactions between ports as nodes in a complex network of shipping, maritime operations, and supply chains create extensive vulnerabilities that simple compliance with CSI, CTPAT, SOLAS, ISPS codes and other WCO and IMB governance protocols would alone not mitigate. Hence, the need for systems-based supply chain-wide scenario and vulnerability management capabilities within ports.

ABOUT THE AUTHOR:
Richard Oloruntoba is an Associate Professor of Supply Chain Management at Curtin Business School, Curtin University, Australia. Richard has 22 years' experience as a logistics and SCM academic in UK and Australian universities. Before academic life, Richard worked in freight forwarding. His research is focused on human and community sustainability in the context of supply chains. He is the Sustainable Development Goal Advisor, Responsible Management, Emerald Publishers UK, and editorial board member of the Asian Journal of Shipping and Logistics.