SECURITY FOR PORTS OF THE FUTURE

Professor Luca Urciuoli,
KTH, Royal Institute of Technology, Stockholm, Sweden
MIT Global Scale Network - Zaragoza Logistics Center, Spain
MIT Center for Transportation and Logistics, Boston, US

Shipping is one of the biggest transport means moving about 80%-90% of the world trade and that has experienced an increased demand from supply chain actors. In particular, the increasing world's real GDP coupled with the globalization trend that aims to move manufacturing facilities abroad in low-cost countries, i.e. India, China and other developing countries, has had a strong impact on the growth of the shipping industry.

As experts in supply chain security claim, increasing flows of goods are attractive targets for criminal groups. The same can be said for the maritime sector, where intentional illicit actions against maritime vessels and port terminals have been increasing in the last few years. Attacks are perpetrated on a global scale and include theft, pilferage, armed robberies, smuggling, piracy, and so forth. Containerized cargo is particularly targeted by criminals and results in theft or smuggling by simply breaking into containers while they are moved on vessels or stored at port terminals. Apart theft, the shipping industry is also exposed to smuggling and therefore law enforcement agencies typically link maritime security to terrorism, drug smuggling, stowaways, human trafficking, and piracy.

Piracy has gained the attention of the international media of late after attacks proliferated in the Gulf of Aden and Somalian territorial waters. This area crosses an important trading route linking Asia to Europe and the US where huge amounts of cargo pass through every year. According to the Suez Canal Authority (2017), in 2017, 17 550 vessels made full transit through the canal two directions, consisting into approximately 1.04 billion tons of freight. Hence, delays and costs to free the hijacked cargo sparked the reaction of shipping and manufacturing companies, and ultimately the NATO military intervention.

CYBERSECURITY

Cybersecuriy and resilience are nowadays such important issues for supply chain and port operators. Information and Communication Technologies (ICTs) are relevant to optimize port management, its operational routines (e.g. processes, production, distribution et cetera) as well as to guarantee the well-functioning of automated handling systems. However, they can be easily exploited to facilitate and perpetrate illicit actions or simply to jam operations.

Experts have pointed out that hacking techniques such as phishing and key-logging could be used by hackers to target pre-cleared containers stored at port terminals. Thereafter, by means of insiders, theft can be performed, or weapons or any other forbidden cargo can be hidden in containers and delivered to a final destination, bypassing cross-border controls. In 2017, a ransomware attack was launched against the Port of Rotterdam, halting operations and causing chaos as well as creating severe economic damage to shipping companies.

CONSEQUENCES OF PORT INSECURITY

Insecurity in ports may have several implications both for supply chain actors and societies. Any flow disruption in a port

implies the loss of assets, goods, personnel and infrastructure damage. It often spreads from the physical carrier or terminal owner, upward to the logistics service provider and thereby to manufactures or distribution actors, with consistent costs and safety implications. The following list attempts to list possible costs, however it should not be interpreted as exhaustive:

- If goods are not delivered on time the supply chain can be forced into a temporary shutdown, ending with lost sales and unfulfilled demand. This implies a productivity loss and overall reduced profits.
- In case of a security breach, part of the loss is covered by insurance but the self-excess is paid by the liable actors. In addition, insurance premiums will inevitably increase.
- A typical reaction to a security breach is to increment protection, leading to increased security costs.
- In case of a security event, due to the multiple actors involved in a supply chain, it may become necessary to determine and assess liabilities. This implies additional costs for the internal audit activities.
- Any suspects accused by investigators will have to be judged prosecuted and detained. This implies additional costs for companies and societies.
- Loss of business reputation. Port terminals affected by security problems may lose credibility and reputation. Supply chain actors could decide to adopt different entry ports into a country.
- Injuries and health danger for personnel. During a security attack, personnel in ports could suffer injuries or life loss, depending on the degree of violence used. In some extreme situations personnel's families could be kidnapped and kept as hostages in order to secure insiders support.
- Ransoms costs. Criminals could hijack cargo and request for ransoms in order to release it to the owner.
- Societal safety. Any terror related threats in port terminals may also put in danger society. Vessels could be used as weapons against residential areas close to port terminals. Containers stored in port terminals could leak toxic gases or contain weapons of mass destruction. This also exposes the surrounding population to health risks and ultimately could damage the transport infrastructure, lowering accessibility and emergency operations.

THE MULTI-ACTOR APPROACH

Maritime and port operations belong to global supply chain operations. Hence, several actors jointly synchronize, move and take responsibility of cargo. When containers

are discharged into ports, they will be temporarily stored in the port terminal, hence under the liability of the infrastructure owner. Thereafter, they could move to a free trade area controlled by customs officers and ultimately to a terminal operator, before being shipped inland to final destination or transshipped onto another vessel.

Hence, port security needs to consider the interaction between different companies and the public. For the same reasons it cannot be heightened with the isolated actions of port operators alone, whether these consist of new technologies or operative routines. Port security is inevitably part of a more complex system where supply chain actors interact and should responsibly ensure that cargo will safely reach its final destination. For this reason, the following recommendations can be put forward to managers:

- **Harmonize security** between port terminals, customs posts and shipping actors. Any weaken spot can be exploited by criminals to perpetrate their actions, nullifying any technological investment or heightened security performed by a single actor alone. In particular, security standards should be kept updated and harmonized across actors.
- **Implement a layered approach.** It is important that all layers of the port and maritime infrastructure are properly secured, including Information Systems. In this aspect, it is essential to ensure IT interoperability and provide solutions to issues related to data confidentiality. In addition, to enhance security it is necessary to ensure top management commitment as well as culture and awareness across personnel. In particular, adoption of risk management frameworks where security is thoroughly considered is essential.
- **Ensure public–private partnerships.** Especially port terminals may benefit to improve cooperation with customs agencies as well as law enforcement agencies. This may support security prevention, recovery and therefore port resilience. ICT (Information and Communication Technology) systems could be used to exchange crime intelligence and support security manager in preparing against imminent attacks. In addition, it is recommended to follow any upcoming regulations issued by the IMO.
- **Interoperability.** Partnerships should focus on the implementation of ICT systems to exchange data with public agencies but also between port operators and supply chain actors.

ABOUT THE AUTHOR

Luca Urciuoli is Associate Professor at KTH Royal Institute of Technology,. He is also Adjunct Professor at the MIT - Zaragoza Logistics Center (Zaragoza, Spain), and research affiliate at the MIT Center for Transportation and Logistics (Boston, US). In the past, he has been working for the Volvo group as a project manager developing telematics services in the areas of transport and logistics optimization, security, and uptime management and diagnostics. He also led the research of the Cross-border Research Association in Switzerland and collaborated in several consultancy and research projects, with a focus on topics like e-Customs, trade facilitation, supply chain security, waste and postal supply chains. Dr. Urciuoli's publications have appeared in several prestigious peer-reviewed journals and he has been an invited speaker to several conferences and roundtables organized by international organizations like the World Customs Organization, the World Bank Group, etc. His research interests includes supply chain management, transport security and risk management, trade and logistics, biomass supply chains.