The Corporate Silk Road

A new era of (e-)infrastructure in Europe?

Smart security in Catalan ports

ENCO EUROPEAN NETWORK OF CORPORATE OBSERVATORIES

ODHE Observatori de Drets Humans i Empreses a la Mediterrània

SHOCK MONITOR

ENCO
EUROPEAN NETWORK OF CORPORATE OBSERVATORIES

ODHE Observatori de Drets Humans i Empreses a la Mediterrània

SHOCK MONITOR

www.corpwatchers.eu/en/investigations/the-corporate-silk-road/
www.odhe.cat
www.shockmonitor.org

Published by the European Network of Corporate Observatories (ENCO), on behalf of Observatory of Human Rights and Business of the Mediterranean Region (ODHE) and Shock Monitor-Observing Private War Impact on Human Rights, initiatives empowered by Suds and Novact, and with the support of Barcelona City Council.

Cover image: PX Fuel

Caterina Zepnova, Nora Miralles and Felip Daza,
Observatory of Human Rights and Business of the Mediterranean Region (ODHE) and Shock Monitor-Observing Private War Impact on Human Rights.

Around 90% of the global trade in goods is carried out through maritime transport. Within this framework, ports are strategical hubs that maintain the global supply chain functioning. Shipping is a priority for the EU economy; around two billion tonnes of cargo are loaded and unloaded at EU ports, while one billion tonnes of oil transit through EU ports and EU waters1. For this reason, the EU and the Member States are steadily innovating in maritime and port security.

Ports of Catalonia are key hubs in the Mediterranean Sea. In 2018, the Port of Barcelona reached total traffic of 67,7 million tonnes, being the Chinese businesses its key partners in terms of exports and imports. In the past years, the performance boost of the Port has been heavily dependent on Asian markets, with elements such as the new container platform BEST and the 2021 recovery plans designed by the Port authorities. These plans include an array of new agreements with Asian ports to be the main gateway of goods and materials of the Chinese giant[2]. In parallel, the Mediterranean corridor and the future European Transport Network (TEN-T) will increase the distribution of materials, goods and services across Europe from the Catalan ports.

1 See: www.ec.europa.eu/transport/modes/maritime/security_en

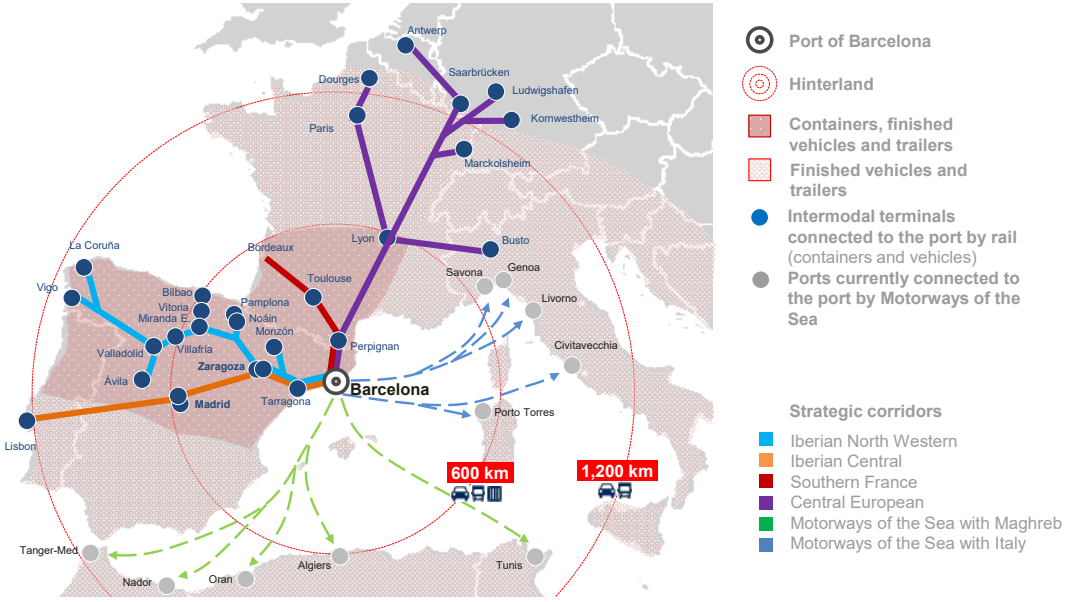
2 See: www.cadenadesuministro.es/noticias/el-puerto-de-barcelona-negocia-ser-la-puerta-de-entrada-a-europa-de-un-puerto-asiatico/

With these new challenges, Catalan ports are becoming leading innovators at the international level via the digital transformation of the ports' services and infrastructures. In this framework, port security plays a crucial role to protect this critical infrastructure and ensure its performance, especially after the 2017 cyberattacks on the Port of Barcelona.

The goal of this paper is to analyse the port security models in Europe using as a case study the Port of Barcelona, but including also references to the Port of Tarragona, the second-largest in Catalonia. With this goal, the structure of the document is the following:

1. Analysis of the evolution of the applicable legal framework closely connected with the transformation of threats and risks;
2. Description of the security ecosystems of Catalan ports including the primary security companies operating and the technologies they employ;
3. Identification of the controversial aspects of this model and the corporate-related human rights impacts.

Location of Port of Barcelona customers and hinterland



Source:
http://portalcip.org/wp-content/uploads/2019/04/16_30_18_05_1_JORDI_TOREENT.pdf

1 Legal framework overview: the evolution of threats

Ports are considered critical infrastructure for the provision of good and materials, and the functioning of essential services in society, such as the energy, chemical and transport services. Thus, prevention of any negative impact on their operations is a priority at the international and national levels. Regulatory modifications of the protection of critical infrastructure evolved in line with the evolution of threats.

The 9/11 attacks in the US caused a turning point in both the international security and national homeland security paradigms. The fight against terrorism implied the securitization of many sectors, including the protection of critical infrastructures. As a result, in 2004 the European Commission adopted a communication on "Critical Infrastructures Protection in the fight against terrorism", calling the European Council and the Parliament to develop a comprehensive strategy for that purpose. In 2008, the EU adopted **Directive 2008/114/EC**, which creates a common framework for the definition and protection of the European Critical Infrastructures (ECI). In 2006, the EU implemented the **European Programme for Critical Infrastructure Protection (EPCIP)** to facilitate information sharing and provide a package of measures for the protection of the ECI among the Member States and other stakeholders. These include the Critical Infrastructure Warning Information Network (CIWIN) and the European Reference Network for Critical Infrastructure Protection (ERNCIP). Both of them are engaged in the analysis of **chemical and biological threats; early warning zones; radiological and nuclear threats; applied biometrics for security; video surveillance and digital; explosives detection**; amongst others. In 2009, the European Commission launched the EU initiative on Critical Information Infrastructure Protection (**CIIP**) to enhance the resilience of ICT systems and networks to any potential disruptions. The initiative promoted a European Public-Private Partnership for Resilience[3].

At the maritime security level, in late 2002 the incorporation of the Ship and Port Facility Security Code (ISPS Code) modified the International Convention for the Safety of Life at Sea (SOLAS). The ISPS Code included specific requirements such as the development of security plans, designation of officials and security equipment.

3 See: www.enisa.europa.eu/news/enisa-news/conclusion-for-the-european-public-private-partnership-ppp-for-resilience-scheme

These international legal changes also tried to respond to the increasing number of **piracy incidents and hijackings** of vessels from 2000[4]. The EU shipping, in particular, was affected by piracy incidents in the Somali coast (Gulf of Aden) in 2005, a geostrategic region for the international maritime transport between Europe and Asia.

In 2004, the EU adopted the **Regulation 725/2004** on enhancing ship and port facility security harmonized with the International ISPS Code. In this way, the European Commission attempted to confront the piracy threat: "*The security of European Community shipping and of the citizens using it and of the environment in the face of threats of intentional unlawful acts such as acts of terrorism, acts of piracy or similar, should be ensured at all time*"[5]. Considering that the scope of the regulation 725/2004 were security measures on board of vessels and the immediate ship/port interface, the EU adopted the **Directive 2005/65/EC** on enhancing port security to protect all the facilities, infrastructures and people within the ports' perimeter defined by the Member States. Additionally, the Commission produced the Regulation (EC) No 324/2008 on procedures for conducting Commission inspections in the field of maritime security. The EU Commission is assisted by the Maritime Security Committee (MARSEC), which provides a mechanism for sharing sensitive information among the Member States.

Also, in 2008, the EU deployed the military operation Atalanta to provide maritime security and ensure the international transportation of cargo, trade and fishing activities in the Horn of Africa[6]. During that period, container shipping companies also contracted Private Military and Security Companies (PMSC) to provide security services to cargo and fishing vessels. The high demand for services in this sector nourished the growth of the private maritime security industry with hundreds of UK, US and Russian companies. But, since 2012, the number of piracy attacks reduced drastically, which led to the disappearance of many maritime PMSCs, and the collapse of the primary Security Association for the Maritime Industry (SAMI).[7] However, piracy-related violence has not been fully eradicated, but has rather shifted from the Gulf of Aden to the Gulf of Guinea and Southeast Asian waters[8]. Moreover, since 2019, the shipping routes in the Arabian Sea and the Persian Gulf have been affected due to an increase in tensions between Iran and the US. In this context, the private maritime security industry has been reactivated and transformed, offering security services to cruises, cargo and port facilities.

4 See: www.icc-ccs.org/piracy-reporting-centre

5 See: www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:067:0013:0026:EN:PDF

6 See: https://eunavfor.eu/

7 Daza, F. (2017). Delimitation and Presence of PMSCs: Impact on Human Rights. In Torroja, H. (Ed.) Public International Law and Human Rights Violations by Private Military and Security Companies. (pp.38). Cham: Springer.

8 See: www.icc-ccs.org/piracy-reporting-centre/live-piracy-map

Catalan ports: hubs of the Mediterranean region

The EU Directive 2008/114/CE was incorporated to the Spanish legal framework through the **Law 8/2011** on the Protection of Critical Infrastructures (facilities, networks, systems, physical and technological equipment of information) from attacks and other threats to ensure the functioning of essential services (transport, energy, financial system, etc.). The Law led to the creation of the Centre for the Protection of Critical Infrastructures under the supervision of the State's Secretary of Security (Ministry of Home Affairs), which coordinates multiple actors, including private corporations as "Strategic Operators" who provide services and goods to maintain critical infrastructures' systems. The Law 8/2011 compels public authorities and strategic operators to develop sectoral strategies and operators' security plans, respectively.

This legal framework contributed to the creation of Public-Private partnership per each sector. In the case of the Ports in Spain, about 170 companies are strategic operators with strong collaborative ties with the public authorities. This cooperation translates into strategic meetings (Cybersecurity thematic group) and joint intelligence and sharing information activities through different digital solutions such as the APP "Alerta PIC" (INCIBE), Reyes and LUCIA (CN-CERT)[9].

The Ports of Spain incorporated the international and EU regulations on port security through the **Law 1617/2007** to improve the protection of maritime transport and ports. Also, the **regulation 704/2011** developed the legislation on the protection of critical infrastructures of ports. Ports of Spain developed a strategic sectorial plan for the protection of critical infrastructures, for specific security plans for each port, and the designation of security delegates. In parallel, the Law 2/2011 of Ports and Merchant Navy regulates the areas of planning, management, delivery of services, economic regime, contracting, and labour conditions within the Ports' system. The regional governments designate the Port's Authority, who integrates the executive functions of each port facility under the supervision of the State's Ports within the Spanish Ministry of Transportation, Mobility and Urban Agenda.

In parallel, an increasing number of piracy attacks to Spanish vessels at the Somali coast forced the Spanish authorities to approve the **Regulation 1628/2009**, which allows PMSCs to use heavy weapons to protect Spanish vessels.

9 See: www.ccn-cert.cni.es/gestion-de-incidentes/lucia.html

But probably one of the most relevant transformations of port security was due to the increasing number of cybersecurity attacks. **Cybersecurity attacks** to critical infrastructures significantly increased, particularly to strategic operators. In 2019, the National Centre for Critical Infrastructures Protection (CNPIC) reported 8.086 incidents (818 to private Strategic Operators and 7.268 to public operators) with different danger and impact levels. From this amount, 50% was related to the financial, energy and transport sectors[10]. These figures crystallize an increasing trend to obstruct essential services using cyberattacks to critical infrastructures: in 2013 there were detected 17 attacks, 50 incidents in 2014, 118 incidents in 2015, 2.569 incidents in 2016, 4.056 incidents in 2017 and 6.954 cyberattacks in 2018[11].

In this context, the Spanish authorities promoted the **Law 12/2018** on Security of information networks. The CNPIC receives support from the National Initiative for Cybersecurity, which also provides support to the National System of Critical infrastructures, including the strategic operators.

Ports and related companies were a key target of cyberattacks. In 2017, the transnational shipping company Maersk was attacked by the virus Petya causing massive disruptions to the international supply chain with $300 million in damages[12]. This intrusion caused the blockage of the fully automated Rotterdam port terminal for one week. The port servers and systems of Barcelona, San Diego and Long Beach were also under attack by the WannaCry and Petya viruses during the same period.

This phenomenon contributed to new researches and investments on digital solutions to deter cybercrime. The Port of Valencia, located in the east cost of Spain, led from 2017 to 2020 the **EU research project SAURON** (scalable multidimensional situation awareness solution for protecting European ports) under the research European programme H2020. Sauron focuses on the integration of physical and cybersecurity systems of the European Union ports. Still, under development, its primary goal is to build an integrated control and management system with new visualization techniques to show and envision the real environment and cyberspace. It will integrate the different control systems and sensors already installed in a port, displaying the situation in real-time in the event of an intrusion or an attack, both physical and cybernetic.

10 Departamento de Seguridad Nacional (2020). Informe Anual de Seguridad Nacional 2019. Ministerio Presidencia del Gobierno de España. (pp.127-135)
Online: https://www.dsn.gob.es/sites/dsn/files/MASTER%20IASN2019%20WEB_0.pdf

11 Idem.

12 Gronholt-Pedersen, J. (2017). Maersk says Global IT breakdown caused by cyber attack. Reuters.
Online: https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO

The government of Catalonia, within its competencies on port's regulation, established two strategic objectives for Catalan Ports: increasing surveillance and access controls; and improving the integration of port-city to enhance the interaction between citizens' activities with ports' infrastructures. In this framework, the Catalan government highlights the importance of executing the dispositions established by the ISPS code and also identifies two main threats to the Ports' facilities in the region: terrorism and accidents such environmental disaster.

2 ——— Security ecosystems: resilience of physical and digital infrastructures

Improving resilience of physical and digital infrastructures has become a new trend in the protection of critical infrastructures. In a context of emerging threats with unconventional attacks (hybrid, cyber-, etc.) directed at vulnerable targets, authorities and security providers have focused on reassuring service continuity in the aftermath of disruptive and destructive events instead of reducing all potential risks at the minimum possible level.

Security plans are preceded by resilience (and cyber resilience) diagnosis of critical infrastructures to identify risks, vulnerabilities, and the capacity of systems, networks and facilities to cope and resist the negative impacts.

Port security authorities are also conducting risk assessments with a resilience perspective to confront multiple types of threats:

- International terrorism, including piracy and cyberattacks;
- Anti-social conducts: vandalism in commercial and leisure public areas;
- Environmental disasters: caused by human activity such as oil spills, waste management, etc.;
- Natural disasters: storms, hurricanes, etc.;
- Organized crime: drug trafficking;
- Irregular migration.

The **European project EMPACT** (European Multidisciplinary Platform Against Criminal Threat), with the participation of the Ministry of Home Affairs of Spain, is an example of the securitization of critical transport infrastructures. EMPACT aims to identify global threats in ports, airports, cities and other transport networks, with particular focus on narcotraffic, illicit arms trade, cybercrime, human trafficking and irregular migration networks.

According to the different nature of threats and targets, port security arranges around two main dimensions: safety and security. These two dimensions get applied to the variety of operational contexts within the port facility and maritime activities: 1) perimeter security; 2) control of access and surveillance; 3) protection of facilities; 4) inspection of goods; 5) maritime rescue; 6) information networks; 7) cybersecurity.

The **Port of Barcelona (PoB)** is one of the major European ports in the Mediterranean region with international commercial relevance[13], and it is managed by the Port Authority of Barcelona (PAB). The Port has the following sectors: Containers and multipurpose terminals (APM Terminals, Terminal BEST, Manipuladora de Mercancías, SL and Port Nou Terminal, SA); Ferry Terminals; Automobile Terminals; Bulk liquids Terminals; Coffee and cacao Terminal BIT; Bulk solids Terminals; Cruise Terminals; Port Vell (public zone); Depot; and ZAL (logistic area).

The Corporative Security Direction manages the port security, which includes three departments: 1) Industrial and environmental security (safety); 2) Operative Security (security); 3) Port police. A Command and Control Centre coordinates all the security activities between these three departments.

The Operative Security Department supervises the port police and the port protection areas. The main goal is to control the port's perimeter to protect people, infrastructures and activities. Among their primary duties, there is the definition of a protection plan under the supervision of Port Authority, with three main objectives: i) to combat the origin of the emergency; ii) mitigate the consequences on people, facilities and environment; iii) reactivate the essential services as soon as possible.

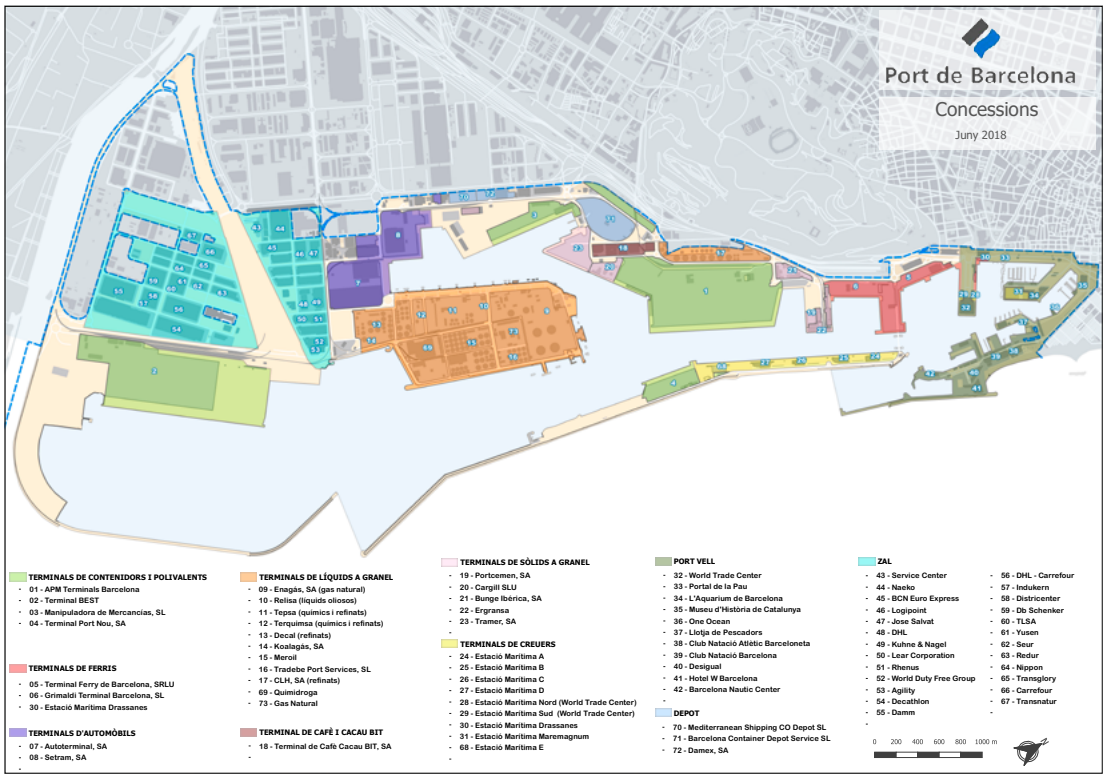
The plan defines specific levels of alert and is integrated into other regional and local security plans defined by the municipalities and public security forces[14]. The Port protection department has the consultative support of a committee with the participation of the PAB, maritime captaincy, representatives of national and local public institutions and police units[15].

The security environment in the Port of Barcelona follows a concentric logic based on circular security areas. In other words, security measures gradually increase from external to central circles. A semi-automatized system executes the control and surveillance activities by regulating the access of people and activities with specific levels of accreditation. The security levels significantly vary between the public spaces (integration city-port) and the most restricted areas.

13 See: https://contentv5.portdebarcelona.cat/cntmng/guestDownload/direct/workspace/SpacesStore/2796db15-57f4-4a9e-8c76-004b4e7e5105/PortBCN_Contenidors.pdf

14 See: http://www.portdebarcelona.cat/es/web/comunitat-portuaria/plan-de-autoproteccion1

15 Baró, B (2010). La Seguretat Operativa al Port de Barcelona. En Secretaria Seguretat (2010). Apunts de seguretat. (Nº 8, pp.49) Barcelona: Generalitat de Catalunya. Online: https://interior.gencat.cat/web/.content/home/010_el_departament/publicacions/seguretat/apunts_de_seguretat/docs/apunts_8.pdf



Map of Port of Barcelona. Source: http://www.portdebarcelona.cat/es/web/el-port/mapa-guia

In this framework, the port's security is a combination of human, physical and logic interrelated areas. It is coordinated by the Command and Control Centre according to the security plans organised in levels of protection of people, infrastructures and the environment.

The human level is a combination of public and private security agents. Public security forces are organised in the port's territory according to three main zones: public (Port Vell), commercial (boarding and disembarkation of passengers) and logistic activities (ZAL). Three police units operate in the commercial area and ZAL: Port police (control of access to restricted areas, special transports, etc.); Guardia Civil (control of passengers, customs control, etc.); National Police Guard -CNP- (border control). Additionally, the regional police unit (Mossos d'Esquadra), together with the local police of Barcelona, operates as integral police in the public zone and is mainly in charge of controlling the transit and mobility around the port. Private security guards support the public security forces by providing complementary services in all these areas. It is important to note that security guards are obligated to inform CNP of any incidents, unusual activity or any other relevant information in terms of security.

The physical level is characterized by a perimeter security detection system with modern surveillance systems, intelligent fences with detection sensors, access control systems integrated with specific degrees of accreditation to access the multiple circles of security, and an alarms

system. Specific gates include OCR/LPR systems that read vehicle plates and verify people's identity and accreditation connected to the SIAM. In the commercial zone, X-ray systems and metal detectors control passengers and baggage. Meanwhile, the ZAL zone is equipped with X-Ray for the inspection of containers (Project Container Security Initiative) and with a system to detect Nuclear, Radiological, Biological and Chemical (NRBQ) threats (Project Megaports).

The logic level aims to prevent, deter and respond to cyberattacks while ensuring the digital transformation of the port. In the Port of Barcelona, there is a broad network of optical fibre and sensors IoT for collecting information from sea, land and air[16].

Recently, drones have been authorised and used to identify the damages caused by the storm Gloria at the external facades of the Port of Barcelona. Barcelona's port authorities are planning to extend the use of drones for surveillance, data collection and maintenance of port facilities[17]. The current regulatory framework opens the possibility to use drones at ports and according to some experts, this type of technology could have a positive impact on port efficiency and the prevention of potential risk but also poses security challenges due to their close location to cities and the airport[18].

The **Port of Tarragona (PoT)** has access to petrochemical facilities in the South of Catalonia. The port is divided into a logistic zone with the capacity of 1,5 million tonnes, a commercial and a sports zone. The industrial sector of the port specializes in the distribution of materials, goods and services, including oil, chemical products, vehicles and agricultural products. PoT is aiming to strengthen its connection with the Mediterranean Corridor through their railroads and the UIC gauge, part of the European Transport Network (TEN-T).

The security system is organized by lines of defence: 1) Perimeter Intrusion Detection System, composed by intelligent fences (7km) and access control system; 2) hundreds of video surveillance cameras; 3) Sealine monitoring cameras. The physical and digital security system is embedded in the Physical Security Information Management system (PSIM) of the Command and Control Centre at the Port police facilities.

16 Sayol, I. (2015). Smart Port, un futur molt present. [Blog post]. Ignasi Sayol. Online: https://ignasisayol.com/smart-ports-un-futur-molt-present/

17 Data obtained from interview with Carles Rúa, Chief of Strategic and Innovation project of PoB, and Catalina Grimalt, Chief Information Officer of PoB on 02/11/2020.

18 Piernext (2019, October 1st). Air drones for port management: effective tool or unnecessary tool? [Blog post]. Online: https://piernext.portdebarcelona.cat/en/technology/air-drones-for-port-management-effective-tool-or-unnecessary-risk/

Smart Ports

Ports are becoming smart cities that provide interactive services to increase efficiency and optimization of resources by using disruptive technologies for the digitalization, automatization, connectivity, monitoring and Artificial Intelligence (AI) to manage transport and logistics.

The Port of Barcelona is a leading actor in innovation and smart ports at international level. The Port Vision 2040 defines 6 areas of innovation with the support of technology: governance, environment, mobility, logistics, people and economy. This model is an adaptation of the Smarty City model defined by the city of Barcelona[19].

The Smart Port of Barcelona works through the **system PortIC**, a traded company with public and private investment. It provides three services via three technological companies, forwarding agents, customs agents, freight hauliers, shipping agents, terminals and stevedores. In particular:

Multi-carrier e-commerce network for the ocean shipping industry. Some of the partners are **INTTRA** in cooperation with **China Ocean Shipping Agency Xiaman, Shenzen EDI Co. Ltd, Shenzen Zsoft Software Development Co. Ltd., Sinotrans Ltd**.

World-leading network for multi-enterprise supply chain orchestration, implemented by Infor Nexus. The network connects businesses to their entire supply chain—from suppliers and manufacturers to brokers, 3PLs, and banks—, paving the way for enhanced supply chain visibility, collaboration, and predictive intelligence. Partners: **Tianjin Login Technology Co., Ltd. And Qingdao Assetech Co., Ltd.** (construction); **Armitage Technologies Limited (HK)** (Industrial Manufacturing).

Network's services, clouding and security, implemented by **BT** in cooperation with **CISCO** for cybersecurity measures.[20]

Smart port technologies consist of smart traffic management, marine environment sensors, passengers' guidance, telecommunication infrastructure, digital information, automation, big data, smart parking, smart maintenance, smart building, workplace mobility, climate and pollution sensors. Some of these technologies are Virtual gates with Optical Character Recognition (OCR) readers and License Plate Recognition

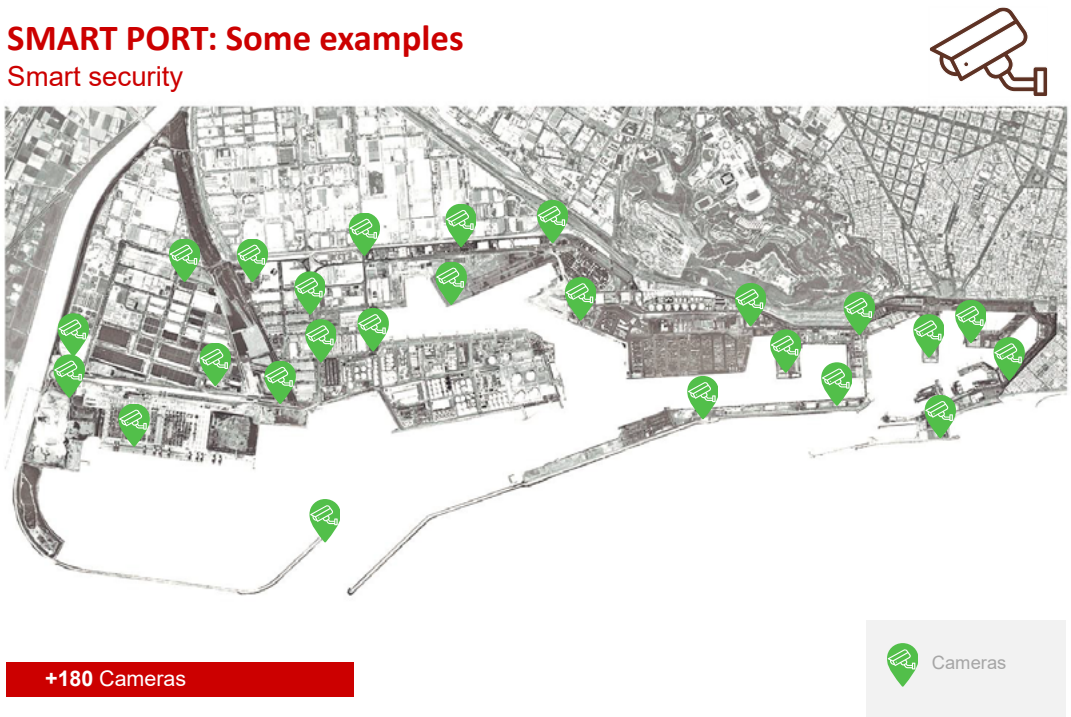
19 Rúa, C. (2018). Port of Barcelona Innovation Model. Pier Next. Online: https://piernext.portdebarcelona.cat/en/governance/port-of-barcelona-innovation-model/

20 Sun, L. (2019). Will Cisco increase its exposure to China buy buying Acacia?. The Mootley Fool. Online: https://www.fool.com/investing/2019/07/10/will-cisco-raise-exposure-china-buying-acacia.aspx

cameras, Trucking PORTal an application to check the traffic situation of the port in real-time and the Power to Ship which implies the electrification of piers[21].

The Governance dimension of Smart Port of Barcelona includes smart security to prevent and deter any threat which can cause an alteration of the supply chain. Considering the increasing number of cyberattacks, physical and digital security integration has become a priority and has created a new layer of security: the logic spectrum.

Smart security provide technologies that integrate internal and external systems and processes into a unique platform. The technology PSIM (Physical Security Information Management System) is an autonomous system that automatically responds to any risk without human intervention.



Map of Port of Barcelona with cameras' location.
Source: *http://portalcip.org/wp-content/uploads/2019/04/16_30_18_05_1_JORDI_TOREENT.pdf*

21 PierNext (2014, November 14th). Smart Ports, in line with Smart cities [Blog Post]
Online: https://piernext.portdebarcelona.cat/en/technology/smart-ports-in-line-with-smart-cities/

The security and safety levels, also, include perimeter intrusion sensors, connected emergency services, video analytics and cybersecurity[22]. Port authorities have displayed hundreds of sensors and cameras to control the territory, people and the situations within the port and its external areas (weather conditions, transit, etc). Modern cameras within the PoB include License Plate Reading, thermal imagining and video analytics. In other Spanish ports such as Tarragona, apart from LPR and video analytics for intrusion detection, AI cameras incorporate facial recognition technology.

Likewise, the Smart Port system does not contribute to the sharing information process between public and private security actors. The sharing of information can happen for major or extraordinary issues (such as pictures of terrorists), and it is also a common thing to provide and receive information from the National Police[23].

22 See: http://portalcip.org/wp-content/uploads/2019/04/16_30_18_05_1_JORDI_TOREENT.pdf

23 Data obtained from interview with ICTS' responsible in Barcelona on 27/10/2020

3 —— Investors and security companies

In the port of Barcelona, terminals all vary in their functionality, most of them intended for cruise ships. The following part maps security companies and technologies by port areas (public, commercial, ZAL and container terminals). For this purpose, it is relevant to highlight the procurement of security services and products conducted through public and private tenders organized by the owner of each terminal.

As previously mentioned, the primary authority in the Port is PAB and possesses a relative degree of autonomy and management freedom. PAB is composed of Spanish State members, Generalitat de Catalunya, Barcelona and Prat de Llobregat City Council, The Barcelona Chamber of Commerce, the Association of Stevedoring Companies and the CCOO and UGT trade unions.

However, even though the Port of Barcelona is a public organism, private, national and international influences are a relevant player in this scheme. Port of Barcelona has received investment from **Hutchison, Gas Natural Fenosa, Grup Acciona (Transmediterrania), Grup Matutes, MSC Cruceros, Carnival and Merlin Properties**. According to a research made by the Catalan journalist Sergi Picazo in 2018, China was the main imports and exports business partner of the Port[24]. It has also been engaged in a high number of contracts with large Chinese construction companies[25].

Other major investors are of Russian origin. In 2010, **Litasco (a subsidiary of Lukoil) and Meroil** (Spain) agreed on a joint venture project, thus giving place to Meroil Tank. This new terminal is now being used to re-export and distribute diesel, biodiesel and jet fuel in Spain[26]. According to Lukoil's website, "the new terminal is equipped with state-of-the-art protection and monitoring systems and is certified for compliance with the international QHSE Management System". As for its reputation, Lukoil has been mentioned in corruption cases in Bulgaria[27], and in 2010, together with a Chinese company Zhuhai Zhenrong (tied to the CCP) , it was involved in the provision of fuel to Iran. Lukoil's directives also have a close relationship to the Kremlin[28].

24 Picazo, S. (2018, July 1st). El Port de Barcelona sota la lupa: negocis, conflicts amb l'Estat i l'ombra del 3%. Crític. Investigació. Online: https://www.elcritic.cat/investigacio/el-port-de-barcelona-sota-la-lupa-negocis-conflictes-amb-lestat-i-lombra-del-3-10505

25 Ídem

26 Lukoil (2012) ЛУКОЙЛ в Королевстве Испания. Lukoil.
Online: https://lukoil.ru/Company/BusinessOperation/GeographicReach/Europe/lukoilinspain

27 WikiLeaks (2011). [OS] BULGARIA/RUSSIA/ENERGY/GV - Bulgarian Customs Agency Inspects Lukoil on Suspicions of Tax Evasion. Global Intelligence Files. Online:
https://wikileaks.org/gifiles/docs/21/2105816_-os-bulgaria-russia-energy-gv-bulgarian-customs-agency.html

28 WikiLeaks (2013). RE:Rep. Global Intelligence Files.
Online: https://wikileaks.org/gifiles/docs/12/1258486_re-rep-.html

Security companies and technologies

In the **ZAL (Logistic Activity Zone)** and the restricted area, they mainly rely on surveillance and cybersecurity companies to guarantee the security of their locations. The ZAL is mainly in charge of attracting maritime traffic with services of logistics infrastructure. It has two main shareholders (Barcelona's Port Authority – 51.5% and Merlin Properties – 48.5%), and it is home to a variety of companies, from supermarkets to petrochemical plants.[29] It is divided into two interconnected logistic areas, where P33 and P42 are the two accesses to and from the port area[30].

Map of ZAL in Port of Barcelona.

Source: Port of Barcelona

ZAL is centrally controlled by the operator **CILSA (Centro Intermodal de Logística, S.A., S.M.E.).** According to a public document published by the PoB[31], ZAL's Security service Centre (consisting of different security products such as CCTV with standard videorecorders) is managed by **Dorlet**. Security cameras providers are **Axis Communications** and **Indra Sistemas**. Access control is provided by the KABA system, a system in charge of operations and customers relations.

29 See: http://www.zalport.com/en-us/who-we-are/about-the-zal-port.html

30 See: https://procseu.portdebarcelona.cat/VentanaDescargaFichero.aspx?vurn=kj5aKBHbEY2wvQYHTU6jRWEvHtrH9jSXTgvn1lepCwxJiypAE3v+Rm4Ag+dl5rlW&vnomfitxer=36306-06-20161545112-2015_000003-2014R32_0023_Proyecto_TIC_accesos_ZAL_Pliego_tecnico.pdf

31 Idem.

Apart from that, ZAL Port has been working with several companies to cover all the physical and cyber security needs. We were able to identify 5 main providers:

- **ELECNOR, S.A.:** this Spanish company has its HQ in Madrid. They signed the latest contract with the Port of Barcelona early in July of 2020[32]. The Port hired the company to implement an expansion project on the system and accesses control to the Logistics area. This company is relevant in the infrastructure, renewable energy and technology sectors. They provide a wide variety of services, ranging from power generation to construction. Despite their initial transparency with all the projects they are currently involved in, there is no mentioning of the Port of Barcelona on their website, nor of any other activities related to ports. Based on the published tender, we can assume that an "accesses control" project is related to the services they offer under the category of Security Systems. ELECNOR can provide CCTV, image analysis and perimeter protection, as well as the centralization of platforms and systems[33]. They mentioned on their website that ELECNOR relies on technologically enhanced security cameras with video analytics, a software that usually includes software recognition features.

- **Securitas Seguridad, S.A.:** owned by the Swedish company Securitas AB, renovated its contact with the Port of Barcelona in July 2020[34]. It provides physical security, monitoring and control of the ZAL area, specializing in alarms and a surveillance system. One of the most versatile companies, in the PoB it is mainly involved in the correct implementation and functioning of the Smart Port System[35]. According to their blog, Securitas Seguridad in the main ensures the protection and management of emergencies. They provide different services, such as securitas Location - real-time monitoring, history of routes, heat maps -, and securitas Connects: in charge of the integral safety management. It improves the security of access controls and internal transits through HD cameras, real-time communications, physical surveillance and containers control. Securitas Seguridad S.A. provides a variety of services to ports, such as Remote Control through the Securitas Operation Centre. Although they do offer video analytics services, the company mostly relies on physical people to carry out its security services.

32 ZAL Port. Ampliación del sistema de control y accesos a la ZAL Port. ZAL Licitaciones. Online: http://www.zalport.com/es-es/licitaciones/licitaciones-adjudicadas/2021004-ampliacion-del-sistema-de-control-accesos-la-zal-port.html

33 Elecnor. (2020). Telecommunications and Systems. ELECNOR-Business. Online: https://www.elecnor.com/telecommunications-and-systems

34 ZAL Port. (2020) Seguridad, vigilancia y control de la ZAL Port. ZAL Licitaciones. Online: http://www.zalport.com/es-es/licitaciones/licitaciones-adjudicadas/2012003-seguridad-vigilancia-control-de-la-zal-port.html

35 Securitas. (2018). Smart Port y la seguridad del futuro portuario [Blog post] El Blog de Securitas. Online: https://elblogdesecuritas.es/smart-port-y-la-seguridad-del-futuro/

- **VOID Sistemas:** Spanish company with its HQ located in Madrid. The contract with the Port was signed in June 2020[36] for compound control purposes, specifically the creation of a massive alerting system for emergencies. VOID Sistemas focuses on the provision of technical services such as phone control, communications recording and alerting. It provides its services to both the private and public sectors. Although not explicitly mentioned, in the PoB it was probably in charge of implementing the new ALERT24 system, released on the market in 2015[37]. The main goal of this system is the massive message sending in case of an emergency. It allows for better coordination of people and services with real-time monitoring.

- **IKUSI, S.L.:** Spanish technological company which HQ are in San Sebastián. It was hired on several occasions by the PoB, the latest being in June 2020[38]. The Port hired the company to supply specific materials and components for the execution of corrective maintenance in the access controls. In 2010 the company also performed the project of "Port security and access control of the PoB"[39], therefore, being the current contract the project's continuation. IKUSI belongs to the VELATIA group, a technological and industrial company. According to its website, IKUSI oversees technological development, helping companies to achieve digital transformation and to modernise. It mostly provides IT, telecommunications and engineering services. Its main goal in the PoB is to efficiently implement (together with other companies) the "Smart Port" project, therefore unifying the different existing systems. Their contribution to the project is through access controls, as they aim to erase the "physical barriers" of access. This system entails a new format of surveillance through digital surveillance. The entrances remain under digital control due to real-time cameras. This system is equipped with vehicle registration plate readers and then fact-checks with the supplied databases about merchandise, personal access points, etc.[40]

36 ZAL Port (2020). Sistema de aviso masivos para emergencias en el recinto de la ZAL Port. ZAL Licitaciones. Online: http://www.zalport.com/es-es/licitaciones/licitaciones-adjudicadas/2022002bis-sistema-de-aviso-masivos-para-emergencias-en-el-recinto-de-la-zal-port.html

37 InfoDefensa. (2015). "VOID Sistemas lanza la nueva versión de su sistema de alerta en emergencias ALERT24." InfoDefensa.com. Online: https://www.infodefensa.com/es/2015/05/08/noticia-sistemas-lanza-nueva-version-sistema-alerta-emergencias-alert24.html

38 ZAL Port (2020). Contrato marco para el suministro de materiales y componentes necesarios para la realización del mantenimiento correctivo en los controles de accesos de la ZAL Port. ZAL Licitaciones. Online: http://www.zalport.com/es-es/licitaciones/licitaciones-adjudicadas/2022007-suministro-componentes-controles-accesos.html

39 Ikusi (2010) Ikusi implementa un sistema de identificación de vehículos y conductores del Puerto de Barcelona. RFIDPOINT. Online: http://www.rfidpoint.com/ikusi-implementa-un-sistema-de-identificacion-de-vehiculos-y-conductores-del-puerto-de-barcelona/

40 Ikusi (2018). Access Control Systems: Drivers behind Port activity. Ikusi Velatia. Online: https://www.ikusi.com/en/blog/access-control-systems-drivers-behind-port-activity

- **PYCSECA:** Spanish company with its HQ in Madrid that provides custody, security and protection services. They operate both in private and public sectors. ZAL's management company, CILSA, signed a contract with PYCSECA in 2017 and until 2020. According to it, PYCSECA is currently in charge of physical monitoring of the perimeter, management of emergencies, control of parking areas and coordination with the public Security Bodies[41].

Regarding the container terminals, in 2012, Hutchison Port Holdings (HPH) acquired BEST (Barcelona Europe South Terminal) for 500 million euros in investments, as the company wanted to transform Barcelona into the main door for the Asian market. Initially, HPH and the operator Tercat (Terminal de Catalunya SA) shared the project, but in the end, HPH became the whole owner of both the Terminal and the operator.[42]

HPH is part of **Hutchison Whampoa**, Hong Kong's largest multinational conglomerate which HQ is currently registered in the Caiman Islands. It has a wide range of investments in a variety of sectors, such as cosmetics, properties, telecommunications and port operations.[43] Over the last decades, the company was under strict control, as the Department of Defence of the USA and others were not sure if Hutchison Whampoa had some connections with the CCP. The former CEO Li Ka-Shing did have at some close ties with the communist party, however, these drastically deteriorated with the presidency of XI Jinping[44]. Additionally, the Department of Homeland Security conducted a meeting with Li Ka-Shing in 2006[45] where the latter promised full willing cooperation.

HPH's BEST Terminal is part of the Mediterranean mega-corridor, serving as an entrance point to both the European and Latin American markets. According to BEST's website, the currently existing security system consists of fences, CCTV, restricted areas, access control, OCR, radiation Detection in the containers, private security Personnel, security Plan and internal Policy[46].

41 CILSA (2017). CILSA licita el servicio de seguridad, vigilancia y control de la ZAL Port. ZAL Port. Online: http://www.zalport.com/es-es/actualidad/sala-de-prensa/notas-de-prensa/cilsa-licita-el-servicio-de-seguridad-vigilancia-control-de-la-zal-port.html

42 Serra, J., Ortega, M. (2012) El port estrena la millor terminal del Meditaerrani per mirar a l'Àsia. Ara.cat. Online: https://www.ara.cat/societat/estrena-millor-terminal-Mediterrani-Asia_0_782321835.html

43 USCC Research Staff (2011). The National Security Implications of investments and products from the PRC in the telecommunications sector. US-China Economic and Security Review Commission Staff Report. Online: https://www.uscc.gov/sites/default/files/Research/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf

44 Lasseter, T., Master, F., Jim, C., Zhai, K. (2019 November 27th). Special Report: How JK's greates tycoon went from friend of China to punching bag. Reuters. Online: https://www.reuters.com/article/us-hongkong-protests-tycoons-special-rep-idUSKBN1Y11LE

45 WikiLeaks (2006). Secretary Chertoff's meeting with Cheung Kong Chairman Li Ka-Shing. Public Library of US diplomacy. Online: https://wikileaks.org/plusd/cables/06HONGKONG1470_a.html

46 Neither the Security Plan nor the Internal policy are provided anywhere on the website.

The BEST Terminal also uses its own Terminal Operating System: nGen. Developed by HPH in 2003, they describe it as "the nervous system – the brain, spinal cord and network of nerves"[47].

- **ICTS Hispania, S.A.** provides the security services in the BEST Terminal. ICTS Hispania is a local branch of the international company ICTS Europe Group. The Group was initially founded in Israel, being the executive direction of ICTS Europe still from this country. ICTS Hispania, S.A. has the latest contract with BEST Terminals since July 2019 and is in charge of a 24/7 control room monitoring[48], access control as well as foot patrol. This company has also been present in Barcelona's Cruise Port Terminal. Its local HQ is in Madrid, while on the international scale their main office is in Belgium. Within the Maritime Safety Services, ICTS Hispania offers a variety of services, out of which the most notable are[49]: hiring and training of security personnel; customers' protection via X-ray machines and metal detectors; CCTV and Valla Smart; foot patrol; vehicle control; emergency plan. On the ICTS Europe webpage, there is a clear emphasis on the need for securing the ports against terrorists and criminal organizations. The company is highly present around the European and the African continents, lately focusing its efforts on Covid-19 related issues, such as passengers' temperature control or the implementation of technology for rapid screening of people[50]. Their presence is limited to foot and access controls, as well as the management of Hutchison's particular software system. They usually do not have access to CCTV unless it is an exceptional situation. Other services provided by ICTS in the Port are a Computer Based Training Platform called Eagle – composed of several courses related to X-Ray technologies and the training of experts on screening –, and RASCargo, a Remote Air Sampling for Canine Olfaction, whose canine services are provided by the French company DiagNose[51].

The **APM Terminals** were founded in The Hague, the Netherlands, but quickly became one of the world's largest port and terminal operators. It belongs to the **Maersk (A.P. Møller – Mærsk A/S) Group**, a Danish shipping company whose goal is to simplify the customers' supply chain.

47 See: https://www.ckh.com.hk/upload/attachments/en/journal/Sphere_47_e_ports.pdf.pdf

48 ICTS Europe. (2019 July 15th). New Maritime Security contract sees ICTS presence expand at the Port of Barcelona. ICTS Europe. Online: http://www.ictseurope.com/media/news-pr/new-maritime-security-contract-sees-icts-presence-expand-at-the-port-of-barcelona

49 ICTS Hispania (2014 june 23rd). Servicios de Seguridad Marítima. ICTS Hispania. Online: http://ictsseguridad.com/icts-hispania-servicios-seguridad-martima/

50 ICTS Europe (2020 September 27th). Israeli start-up "Virusight Diagnostic" Signs Strategic LOI with ICTS Europe for COVID-19 Rapid Screening in International Airports around the globe. ICTS Europe. Online: http://www.ictseurope.com/media/news-pr/israeli-start-up-virusight-diagnostic-signs-strategic-loi-with-icts-europe-for-covid-19-rapid-screening-in-international-airports-around-the-globe

51 Data obtained from interview to ICTS Hispania employees in Barcelona on October 27th of 2020.

APM Terminals acquired the Spanish container terminal operator in 2016. According to the company's CEO Kim Fejfer, the main reason for the acquisition was the provision of a "strong gateway presence in Spain"[52].

APM Terminal in Port of Barcelona

Source: ODHE

It is important to remark, that no information about tenders, subsidiaries or subcontractors can be found on the official webpage. We were able to find some news about the Port of Algeciras (Andalucía) that led to the conclusion that Prosegur was the security company that worked for APM Terminals[53], as well as in APM Valencia[54]. No information about the PoB could be found.

- **Prosegur Compañía de Seguridad, S.A.** is a multinational security Company based in Madrid specialized in alarms, security personnel, cash delivery and cyphers. We can only assume that it was hired by APM Terminals to establish an alarm system, as well as guarantee physical and cybersecurity.

52 Bonney, J. (2015).APM Terminals to acquire Spanish container terminal operator." JOC.com. Online: https://www.joc.com/port-news/terminal-operators/apm-terminals/apm-terminals-acquire-spanish-container-terminal-operator_20150908.html

53 Estrecho Digital. 2019. Protestas de la seguridad privada de APM Terminals. El Estrecho Digital. Online: https://www.elestrechodigital.com/2019/04/30/protestas-de-la-seguridad-privada-de-apm-terminals/

54 LinkedIn. Profile of Jordi Barbero Manzano [Linkedin profile]. LinkedIn. Online: https://www.linkedin.com/in/jordi-barbero-manzano-b27896145/?originalSubdomain=es

- **ORBITA Ports & Terminals**, Spanish Terminal Automation Company based in Valencia. It has little to do with Port Security *per se*, however, in 2018 ORBITA conducted an "Automation of the entrance and exit door of the container Terminal with ten lanes"[55]. The project's goal was to increase the doors' efficiency and reduce the human error factor. Based on GateLPR and GateMDG technologies, the system is in charge of automatic license-plate reading and detection of dangerous goods.

Virtual gates with LPR cameras designed and installed by ORBITA in Port of Barcelona

Source: https://www.orbitaports.com/projects/apm-terminals-barcelona/

Regarding the transportation of passengers, the Port of Barcelona is considered the biggest **cruise port** in the Mediterranean, with seven international cruise terminals and two ferry stations. The PoB remarks that safety and security are of the *utmost importance* for the port and that they fully comply with the requirements of the International Maritime Organisation (IMO)[56] .

The increasing number of regular cruise lines has prompted a new security contract between PoB and the already mentioned ICTS Hispania, S.A. since 2014[57]. **ICTS Hispania, S.A.** and **ICTS GENERAL SERVICES, S.L.** (subsidiary which provides auxiliary services) are currently in charge of the provision of security services, control of passengers' flux and luggage inspection. Among the provided port services, the following are particularly noteworthy: **screening of people and personal effects; accesses control and foot patrol**.

55 Orbita (2018). Automatización de la puerta de entrada y salida de la Terminal de contenedores con 10 carriles. ORBITA Ports & Terminals. Online: https://www.orbitaports.com/es/projects/apm-terminals-barcelona/

56 Port of Barcelona (2020). Barcelona Cruise Facilities 2020. Port de Barcelona. Online: https://contentv5.portdebarcelona.cat/cntmng/guestDownload/direct/workspace/SpacesStore/42d44f29-05af-4260-8939-2011bf6bc87c/bcf.pdf

57 ICTS Hispania (2014 October 28th). ICTS MARITIME nuestro comienzo y desarrollo. ICTS Seguridad. Online: http://ictsseguridad.com/icts-maritime-nuestro-comienzo-y-desarrollo/

Furthermore, different cruise and ferry lines have opted for hiring their own security services. Barcelona cruise port operates five public cruise terminals - A, B, C, WTCB North and WTCB South -, and two terminals authorized for Truck-To-Ship (TTS) and Ship-to-Ship (STS) - D Palacruceros and E Helix. Puerto de Cruceros de Barcelona is the company in charge of the management of the cruise terminals[58] .

Several cruise lines operate in the PoB as of 2020[59], the most important are:

- **Carnival Cruise Lines:** All the ships use a visual identification security access system to determine whether an individual is authorized or not inside.[60] The cruise line also relies on facial recognition technology "to make the embarkation and debarkation process faster and more efficient". Each passenger and crew member are taken a photo at the beginning of a journey. This photo gets updated each time an individual leaves the ship. The company claims that they store the pictures only for the duration of the cruise.[61]

  There is barely any information about the security personnel recruiting process and/or company in charge of it. The only information that we could find was the Carnival Support Service India Pvt. Ltd, India's largest crewing company that provides highly skilled and trained personnel for cruise ship operations worldwide. It is in charge of HR-related functions, provision of training solutions and the usage of innovative IT services.[62]

- **MSC Cruises –** In 2017 it launched a new video surveillance system together with **Bosch and Hewlett Packard Enterprise**. It consists of an intelligent video capturing and analysis system with the primary goal of detecting people or objects falling overboard. MSC Cruises describes it as a "comprehensive shield of intelligent optical and thermal video cameras which provide nonstop [...] surveillance alongside the relevant exterior parts of the ship"[63]. MSC's ships also possess 1200 HD CCTV cameras on board. For their onboard cybersecurity, MSC relies on **Palo**

58 Cruise News (2020 July 9th). Barcelona Cruise Port se acredita a nivel internacional como infraestructura segura ante el Covid 19. Cruise News Media Group.
Online: https://www.cruisesnews.es/Portal/2020/07/09/barcelona-cruise-port-se-acredita-a-nivel-internacional-como-infraestructura-segura-ante-el-covid-19/

59 Port of Barcelona (2020). Barcelona Cruise Facilities 2020. Port de Barcelona.
Online: https://contentv5.portdebarcelona.cat/cntmng/guestDownload/direct/workspace/SpacesStore/42d44f29-05af-4260-8939-2011bf6bc87c/bcf.pdf. ; See also: http://www.portdebarcelona.cat/documents/10157/46128724/en.armadors.pdf/d4e19b6a-69c0-4c1a-80f1-fd7c4780a6b4

60 https://help.carnival.com/app/answers/detail/a_id/3966

61 https://help.carnival.com/app/answers/detail/a_id/6019/

62 CSSI. 2020. About us. [LinkedIn profile].
Online: https://www.linkedin.com/company/carnival-support-services-india-pvt.-ltd/

63 MSC. (2017 October 20th). MSC Cruises deploys innovative man overboard detection technology. MSC Corporate Information & Media Room. Online: http://www.mscpressarea.com/en_INT/press-releases/1614

Alto Networks which provides firewalls and centralised management. Another feature of this cruise company is *MSC for Me*, an app that aims to make the customer experience easier and more efficient. One of its features is *TailorMade*, a service that learns about individual preferences to offer customised activities. It does so through **face recognition, geo-localisation and interactive bracelets**, although it is an optional service[64].

MSC uses an external company to select and hire security officers on board. Their current partner is **MS Security & Personnel Ltd**[65], a maritime security company. It deals with terrorism, piracy, stowaways, violence, vandalism, drug trafficking and which offers Passenger *Vessel Security* and *Port Security*. Their list of services is quite extensive, with 24/7 onboard patrolling, testing of security equipment and even the possibility of the use of force as a last resort. To guarantee passenger safety, MS Security and Personnel security guards can also perform, among others, the following operations[66]: performing of computerized and visual identification procedures of crew and passengers in the gangway; risk assessment of entering persons due to suspicious signs and behaviour; operating and monitoring CCTV systems; response team for all types of incidents; investigating and interrogating due to suspicious behaviours; surveillance of a vessel's surroundings.

MS Security & Personnel Ltd also owns two Private Maritime Security Companies to provide specific anti-piracy services to cargo vessels with armed personnel, **Black Pearls and MASS**, in the contexts of Red Sea, Gulf of Aden, Indian Ocean, Gulf of Oman and West Africa[67]. The container shipping area of MSC also contracts security guards of MS Security & Personnel to protect their merchant ships. MSC cargo vessels operate in Spanish ports, Las Palmas (Canary Islands)[68] and Barcelona.[69]

64 See: https://www.msccruises.com/en-gl/MSC-Voyagers-Club/Newsletter/MSC-Cruises-Newsletter-MSC-Smart-Ships.aspx

65 This company is a maritime professional security MSC Cruises. 2020. "Onboard Jobs/Hotel - Security". Careers MSC Cruises. Online: https://www.careers.msccruises.com/#/onboard-jobs/security

66 MS Security & Personnel (2020)Passenger Vessel Security". MS Security & Personnel – Shore Side Support. Online: https://www.ms-security-ltd.com/passenger-vessel-security

67 See: https://www.ms-security-ltd.com/anti-piracy-for-commercial-vessels

68

69 See: https://www.harbourmaster.org/News/msc-sixin-23-656-teu-maiden-call-barcelona-largest-ship-berth-any-barcelona-terminal

- **Royal Caribbean –** Since April 2011 ICTS is in charge of providing security services for passenger and luggage access control, dock security and k9 cargo service in the ports of Malaga and Barcelona[70]. Their services include passenger screening; X-ray of luggage and equipment; and guarding of the terminal and vessel.

  In 2019, Royal Caribbean decided to implement IDEMIA's MFACE technology to increase efficiency and security during the debarkation process. This facial recognition technology matches the faces of individuals with the identities of the ticketed passengers. The company assures that it does not store the pictures after the end of the trip.[71]

  Royal Caribbean relies on **HR Maritime Security (HR-MARSEC)** to provide third-party management services. Founded in Israel, the company ensures sea and land protection, reduces the risks of cyber threats and is in charge of the training process of their employees and clients. HR Maritime Security indicates that their employees come from **military, law enforcement and intelligence services from "both Israel and around the world"**[72]. Among their services, we can find Cyber Security, CCTV & Security Technology, Close Protection and Anti-Piracy & Maritime Security Solutions.

  As for the selection and provision to the ships of security personnel, Royal Caribbean relies on **SEM Maritime Security Group**. Their operatives have all served in the Israeli Defence Forces and are former Royal Marines personnel, being defined as "well-trained individuals, ready to handle any mission they are assigned"[73]. Their services include: counter Piracy Guidance; on Board Security Teams; maritime Intelligence; terminal and Port Risk Analysis; crisis Management/Training, amongst others.

70 ICTS Hispania (2014 September 12th). ICTS Hispania presta sus servicios al Oasis of the Seas, el buque de cruceros más grande del mundo. ICTS Hispania. Online: http://ictsseguridad.com/icts-hispania-presta-sus-servicios-al-oasis-of-the-seas-buque-de-cruceros-mas-grande-del-mundo/

71 Hochberg, M.. (2019 April 16th). Royal Caribbean to expand facial recognition tech to more ports to speed up disembarkation [Blog post]. Royal Caribbean Blog. Online: https://www.royalcaribbeanblog.com/2019/04/16/royal-caribbean-expand-facial-recognition-tech-more-ports-speed-disembarkation

72 See: https://hrmarsec.com/about-us/

73 See: https://www.semsecuritygroup.com/

The **public area** of the Port of Barcelona (Port Vell) is secured by the port police (120 members and 36 auxiliaries), the different Protection Plans and the Advisory Committee (Port Authority and advisory body of Security bodies). The public area is a crucial space for the interaction of citizens with port facilities, which is a priority for the Government of Catalonia. Before the outbreak of Covid-19, thousands of tourists and locals visited the Port Vell to access to multiple services. In this context, during the last years, the street sellers' activities saw an increase in this area, which evolved in tensions with local vendors. The answer from the Barcelona city council was to increase patrolling activities by public security forces. Meanwhile, PAB protected the area with port police units and private security guards from ICTS Hispania[74].

In the port of Tarragona, the Israeli company **Magal Security Systems** has installed a comprehensive perimeter intrusion detection system (PIDS) in the port facilities through several public contracts since 2013 for a total amount of 3.351.091,53 euros[75]. The security system consists of perimeter intelligence fences with intrusion detection sensors; control of access technologies and infrastructure; a CCTV system with 150 modern cameras (thermal, facial recognition and LPR), including video analytics technology for maritime security. The digital and physical security infrastructures are integrated into Fortis 4G, a command and control semi-automatized platform.[76]

74 Data obtained from interview to ICTS Hispania employees in Barcelona on October 27th of 2020

75 ODHE (2019). File's company of Magal Security Systems. ODHE Publications. Online: www.odhe.cat

76 See promotional video: https://www.youtube.com/watch?v=17Yw7HiRjdk

4 Human rights impacts and potential abuses

This final section identifies critical trends on human rights impacts identified from the analysis of the Catalan port security systems. In specific cases, we also identified similar issues in other Spanish ports reinforcing the trends and the structural aspects which contribute to human rights' violations and other potential abuses.

Opacity, isolation from the city and other barriers to accountability for human rights violations

The trend towards securitization of the so-called critical infrastructure materializes through the deployment of huge physical security and cybersecurity measures and access control technologies. This turns civil infrastructures considered critical into opaque fortifications isolated from the rest of the city, where the protection of rights against potential abuses becomes increasingly complicated.

This trend appears closely linked to the securitization of migration, which has moved in the last two decades from the social agenda to being conceived as a major threat to Western states. Since 2001, the implementation of anti-terrorism and security policies in the maritime sector has contributed to the shielding of ports against unwanted intrusions77, not only intending to prevent terrorist attacks or cyber-attacks but also to hinder the disembarkation of undocumented persons and asylum seekers. Despite being justified based on the port designation as critical infrastructure, the opacity in the management of security and its isolation through a perimeter zone, restricted only to people authorized by the Port Authority and protected by enormous security measures, favours the occurrence of potential human rights violations in the facilities of the cargo port and the ZAL's areas. Furthermore, this dynamic also compromises other rights, such as the right to privacy in the face of invasive technologies, the labour rights of people working in port facilities and on ships, as well as the right to peace, since some of the port's security contractors are also involved in the defence and border security industries. In addition to making accountability extremely difficult, opacity prevents possible abuses from going beyond the sensorized fences that surround the facilities and spreading into the

77 Maquet, P., Burtin, J.. (2013 . Statewatch, Sanctions for stowaways: how merchant shipping joined the border police. In Statewatch Journal vol 23 no 2. (London: Statewatch). Online: https://www.statewatch.org/media/documents/subscriber/protected/statewatch-journal-vol23n2-august-2013.pdf

public. The vaunted connection between the port and the city in the smart cities concept thus becomes a technological screen that hides the reality of this growing isolation and makes clear the need for public scrutiny and periodic audits by independent human rights organizations.

Impacts on the human rights of migrants

Opacity means that it is practically impossible to detect and prosecute practices such as those denounced by the NGO Migreurop in a report launched in 2012[78], based on interviews made in 23 ports across Europe, including the ports of Barcelona and Bilbao (Basque Country). The report points out the violation of the rights of people who sneak onto ships to try to enter another country, the so-called stowaways. If a stowaway is found on board of a cargo ship, a merchant ship or a vessel of any kind, many European states consider the charter companies responsible for retaining them and preventing them from escaping, under the threat of a heavy fine. If the stowaway claims his/her right to apply for asylum or to have a doctor, the vessel must remain in port in detention until the migrant obtains a response to his/her request for protection or leaves the hospital, thus delaying the journey.

The treatment of stowaways casts a perfect example of how externalisation of public policies to the private sector works in maritime trade. When the vessel docks in port, the stowaway is usually kept on board by private security companies, with the abuses and impunity this can bring.

Its co-author Julia Burtin claims that in the Spanish case stowaways are often not reported to the police, so no one knows of their existence. This fact can encourage an even more awful practice. When the stowaway's nationality cannot be proven for refoulement -as stipulated by maritime law- or the ship is not going to return to the port where he/her illegally embarked, the report documents several cases in which migrants were thrown overboard and abandoned at sea, locked up in subhuman conditions or forced to work on the ship. Also, in 2004, the captain of a merchant ship moored in La Coruña was arrested for ordering the crew to throw overboard four sub-Saharan migrants travelling illegally on the ship[79]. Also, Barcelona activists denounced in 2015[80] that several workers in the port of Barcelona had confirmed the existence of this practice.

78 Migreurop. (2012). Los confines de Europa. La realidad de los controles migratorios. Informe 2010-2011.

79 La Voz de Galicia. (2017) . El «Wisteria» hizo visible el drama de los polizones. Barbanza. June 15th. Online: https://www.lavozdegalicia.es/noticia/barbanza/2017/06/11/wisteria-hizo-visible-drama-polizones/0003_201706B11C11991.htm

80 Arbide, Hibai.(2015). Narco, politiqueo, trepas y asesinos en el puerto de Barcelona. Playground, January 27. Online: https://www.playground.media/news/narco-politiqueo-trepas-y-asesinos-en-el-puerto-de-barcelona-41841

At the same time, security in the port areas has been reinforced to the extreme to prevent clandestine boarding. Security gets reinforced with the publication of maps showing the different "hot spots" and "risk areas" where the ship is likely to receive stowaways, or with the erection of walls that prevent potential asylum seekers from accessing the ship.

One of the most controversial cases is that of the port of Bilbao, from where passenger and goods vessels chartered by Brittany Ferries set sail towards the port of Portsmouth. After the dismantling of the camps for irregular migrants in Calais, up to 100 stowaways were counted every day. In 2017, the Port Authority built a four-metre-high wall for 230,000 euros and intensified surveillance in the port of Bilbao[81] to stop undocumented migrants from entering the area of trailers, lorries and containers. The Basque government justified the measure by considering the port as critical infrastructure. However, activists in solidarity with refugees and the feminist movement denounced the wall as dangerous for the integrity of migrants and as a contribution to the fortification of European borders, which seriously violate human rights of migrants and potential asylum seekers.[82]

In short, the tendency in the ports, including Barcelona, is to hinder the mobility of migrants while at the same time facilitating the entry of goods.

Invasive technologies, biometric systems and impacts on the right to privacy

The advance of large-scale data connectivity and interoperability and its scope, as well as the use of biometric technologies - which extract data from the human body - and of behavioural analysis, are another of the debates arising from the securitisation of critical infrastructure. Especially, when it comes to the deployment of invasive technologies, such as facial recognition systems (implemented through video surveillance cameras), access controls, number plate controls and in cruise ship landing terminals. These technologies collect sensitive and intimate data, often taken without our explicit permission.

According to EDRI and several other European digital rights organisms, biometric or behavioural analysis technologies can challenge rights such

81 Alonso, J.M. (2018). El otro muro de los inmigrantes: el puerto de Bilbao pone fin a los asaltos de polizones. El Confidencial, December 7. Online: https://www.elconfidencial.com/espana/pais-vasco/2018-12-07/polizones-puerto-bilbao-ferry-inglaterra-asaltos-descenso-drastico_1684754/

82 Reviriego, J.M. (2017). Una marcha de mujeres denuncia el «muro de la vergüenza» del Puerto y el tráfico de armas. El Correo de Bizkaia, December 17.
Online: https://www.elcorreo.com/bizkaia/marcha-mujeres-denuncia-20171217205955-nt.html

as privacy and intimacy[83] by assimilating security and control of citizens. Furthermore, these technologies generate vast databases of sensitive information in the hands of large corporations, governments or international criminal networks. These systems, far from functioning neutrally, reflect social and racial biases. For example, they associate ethnic minorities and racialized people with a greater likelihood of committing criminal acts.

In the context of the Catalan ports, according to an internal source from the Barcelona's Port workforce, there have been attempts in the private part of the port to implement access control systems using fingerprints, which would fall into the category of biometric information. For now, it seems that they have not finally been implemented, due mainly to the irruption of Covid-19[84].

A particularly noteworthy case took place in the port of Tarragona. It deployed - as indicated above – hundreds of video surveillance cameras, potentially including facial recognition systems and video analytics for intrusion detection. The intention of those responsible of the management of the port is to gradually include this type of biometric system into its integrated security device, currently in the hands of the company Magal S3 España S.L., the Spanish subsidiary of Israeli company Magal S3 Security Systems Ltd.

Also, several cruise lines are incorporating potentially invasive security technologies for their passengers. In the Port of Barcelona, some of the operating cruise companies currently leading the implementation of biometric systems on its terminals are Royal Caribbean[85] and Carnival Cruises. The latter, as mentioned above, uses facial recognition technology on passengers and crew members. Last August, a cyber-attack accessed personal data of guests and employees from three branches of Carnival Cruises, exposing the vulnerabilities of these systems in terms of protection of the right to privacy and misuse.

On the other hand, the obsessive commitment of the ports, and especially of the Port of Barcelona, to cybersecurity - partially motivated by these severe computer attacks - configures a way of dealing with the management of large data centred on the notion of national security and not on people[86]. The innovations produced in this field accelerate the deployment of forms

83 EDRI. 2019. Facial recognition and fundamental rights 101. December 4. Edri.
Online: https://edri.org/our-work/facial-recognition-and-fundamental-rights-101/

84 Data obtained from interview with Port of Barcelona workers on November 21st 2020.

85 Larry, B. (2019). Royal Caribbean to Roll Out Facial Recognition Technology for Disembarkation in Select Ports. Cruise Critic. October 10. Online: https://www.cruisecritic.com/news/3993/

86 Liaropoulos, A.N. (2016). Reconceptualising Cyber Security: Safeguarding Human Rights in the Era of Cyber Surveillance. International Journal of Cyber Warfare and Terrorism, Volume 6, Issue 2. April-June 2016

of surveillance and monitoring of everyday life, which are applied not only to deter a potential cyber-attack that could paralyse the activity of the port, as it is argued. They are also used to control the flow and mobility of people, for example, through a collaboration with the European Union's Entry-Exit System. This system will not only see its implementation at the EU's external borders but probably also in the ports with the highest passenger traffic[87]. It plans to deploy biometric technologies to obtain names, passport numbers, fingerprints and photographs of travellers from third countries, data that will be stored for five years.

Labour rights

The aforementioned opacity of the port and the entry of large corporations and investment funds has led to harmful dynamics concerning labour rights. On one hand, docks have been outsourced to transnational companies, leading to the emergence of cases of violation of workers' rights. On the other hand, the mooring and security companies in the Port of Barcelona themselves have experienced labour conflicts and strikes.

Since the 1980s, several strikes have taken place on the perimeter of the Port of Barcelona, the last one in 2017-18 precisely linked with the entry of big financial companies. In this latest case, it was the American company JP Morgan that bought the port logistics services holding Noatum and tried to sell it to a Chinese company without the dockers[88], in line with an attempt at liberalisation that this strategic sector is experiencing. Strikes also took place within companies, such as the mooring company in the Port of Barcelona Mooring & Port Services, for the imposition of sanctions and warnings for refusing to carry out work outside of the agreement and for non-payment of overtime to the port workers[89].

The shipping giant Hutchison Ports Best, relevant for its size and influence as a terminal operator in the Port of Barcelona, is known for the many labour conflicts that have emerged in the 27 countries in which it operates. For example, after Hutchinson's entrance in the ports of in Sydney and Brisbane, the company dismissed hundreds of workers via SMS at midnight. Likewise, a protest of Hong Kong dockers lasted 40 days, demanding the company

87 Eu-LISA. 2019. Entry/Exit System (EES) Working Group on ICT Solutions for External Borders (sea/land) Report. March 26. Online: https://www.eulisa.europa.eu/Publications/Reports/WG%20on%20ICT%20Solutions%20for%20External%20Borders%20-%20Report.pdf

88 Moreno, C. (2018). Lucha obrera, sindicalismo 2.0 y feminismo: una mañana en la estiba de Barcelona. El Salto, February 8.
Online: https://www.elsaltodiario.com/estiba/lucha-obrera-sindicalismo-feminismo-estiba-barcelona

89 Grodira, F. (2018). La empresa de amarre del Puerto de Barcelona rompe el preacuerdo con los trabajadores, que harán tres días de huelga. Público, February 14. Online: https://www.publico.es/economia/guerra-laboral-empresa-amarre-puerto-barcelona-rompe-preacuerdo-trabajadores-haran-tres-dias-huelga.html

to wage raises and to improve work safety[90]. In some subsidiaries of the company in other countries such as Panama, violations of labour rights also were reported.

Privatization of security

One of the most evident trends in port and maritime security is the privatization of security services and areas, whether in access controls to restricted areas of ports or in surveillance on cargo and cruise ships, both in route and at berth. Gradually, private security companies get contracted for different types of activities, including quasi-police tasks, intelligence and training.

After 9/11, the ISPS Code requires security training for shipping companies and port operators. Since then, private security companies offer services to train crews from cruises and merchant ships to prevent access to intruders or stowaways. In a similar trend, the maritime security industry has specialized in intelligence operations by undertaking a risk assessment of port facilities, analysis of risks for international cruises' tour or developing digital platforms to identify and assess the evolution of worldwide security concerns.

In the case of the Port of Barcelona, several security companies operate within its perimeter, most of them providing access to the different areas of the port and carrying out surveillance tasks within the premises. However, their role extends to the cruise terminals, where, for example, ICTS Hispania carries out terminal and mooring security, passenger flow control and luggage inspection. These are all activities traditionally performed by Guardia Civil. In the public area of Port Vell, ICTS Hispania has conducted security activities to prevent street selling, including the support to police interventions. Considering the privatization of security process and the ongoing de-professionalization of the sector, the participation of private security guards in law enforcement activities raises major concerns due to limited public scrutiny and lack of preparation and rules of engagement.

Another critical aspect is that transnational companies have become authentic private armies offering military and security services, which implies the outsourcing of inherent State functions and questions the legitimate use of force. The activities that better reflect this trend is on-

90 Jeune, P. (2018). Hutchison Ports is about to sack 1000 people for the port with no future. EU Today, August 02. Online: https://eutoday.net/news/business-economy/2018/hutchison-ports-is-about-to-sack-1000-people-for-the-port-with-no-future

board security services in cargo vessels to prevent piracy assaults, hijacking and stowaway. Usually, personnel with military and combat experience provide this type of armed services. Indeed, in anti-piracy activities, the PMSC's members engage in real combat operations with heavy weapons. As we observed, a large number of flag states -including Spain since 2009- have authorized the deployment of armed guards, either military or private, aboard merchant ships and tuna boats. In addition to the protection of tuna and other fishing vessels operating in the Indian Ocean and other risky waters, many maritime security companies offer their services in and out of port to merchant ships and cruise ships.

The consequence is the growth of a Private Military and Security industry operating in ports, vessels and other critical infrastructures. The sector characterizes by its opacity and transnational nature, which undermines its public scrutiny. These problems are exacerbated by the lack of international binding instruments to regulate the phenomenon of privatization of war and security in general and the activities of PMSCs in particular.

Companies involved in the defence and border security sectors

The progressive outsourcing of port security associates to the growing presence of security companies, some of which are heavily involved in the defence and border security industries. Furthermore, they operate in contexts of occupation or serious human rights violations.

One of the most severe cases is Magal S3, which manages the security devices of the port of Tarragona. Magal's parent company in Israel is famous for using the Palestinian Occupied Territories and their population as a laboratory for its surveillance technology products during the development phase, which Magal subsequently offers worldwide with the label "Tested in Combat". Magal Security Systems was created in 1969 as a department of the state-owned Israel Aerospace Industries. In 1984 it became a private company but maintained its close relations and contracts with the Israeli Ministry of Defence. Magal is one of the major profiteers of the occupation of Palestine. The company has installed 170km of PIDS worth $15 million in Israel and the OPT, has equipped Israeli prisons where are imprisoned Palestinian political prisoners, and placed its technologies in Israeli illegal settlements in West Bank of Ariel, Alfei Menashe, Karnei Shomron, Shilo, Geva Binyamin (Adam), Tzofim, Shaked, Giva'at Ze'ev, Oranit and Itamar. Magal has become a world leader in PIDS thanks to the gained experience and technologies-testing in Occupied

Palestinian Territories (OPT)[91]. Magal conducted the latest tests during the Palestinian demonstrations in March 2018 against the Israeli occupation in Gaza Strip. In the value chain of Magal, there are other Israeli companies such as Mer Group, who is included in the **UN report A/HRC/43/71** on businesses with economic activities in the illegal settlements in the OPT. Smart-M produced by Mer Group is also a technology used in the "Mabat 2000" panoptical monitoring program in East Jerusalem, composed of facial recognition cameras for mass surveillance and control of Palestinian people.[92]

Many of the companies that develop or supply the technological architecture of the port and its access control systems, such as Indra or Elecnor, are old acquaintances of the arms industry and border surveillance in Spain and Europe. Others, such as Gunnebo, have recently joined these controversial sectors, which are linked to the violation of the human rights of migrants. In the case of Indra, a provider of video surveillance systems at the port, it is one of the primary Spanish contractors of the Frontex Agency and the Integrated External Surveillance System (SIVE) for borders, in addition to being one of the major defence companies in Spain[93]. Elecnor S.A., which has recently received an expansion of the access control system in the ZAL of the Port of Barcelona, and its subsidiary Deimos, highly positioned in the space and satellite engineering field, have received contracts worth almost 3 million euros in defence[94]. Its satellites also have applications for border control and surveillance. In 2018 the company received an award for the maintenance of SIVE[95] .Gunnebo Iberia is a subsidiary of Sweden's Gunnebo Security Group, with a delegation in Barcelona. Recently it became famous for being the company in charge of the renewal of all the security cameras in the 8 kilometres of border between Ceuta and Morocco, which has the primary aim of preventing migrants' attempts of entry.

Another significant case is ICTS Hispania, which depends on ICTS Europe, a company of Israeli origin. It operates in the port of Barcelona and even offers private security services to the cruise ships that dock there. Furthermore,

91 Daza, F. (2020). The Invisible Walls of the Occupation. The traceability of Magal Security Sistems in the (cyber) security supply chains in Israel and Palestine. ODHE/Shock Monitor
Online: http://www.odhe.cat/es/los-muros-invisibles-de-la-ocupacion-la-trazabilidad-de-los-productos-de-magal-security-systems-en-las-cadenas-de-suministro-de-la-ciber-seguridad-en-israel-y-palestina/

92 Miralles, N. (2020). The privatization of security, social control and gender impact on East Jerusalem. ODHE/Shock. Online: http://www.odhe.cat/es/privatizacion-de-la-seguridad-control-social-y-su-impacto-de-genero-en-jerusalen-este-2/

93 Infodefensa .(2020). INDRA vuelve a ser la únicae mpresa espanola en el top 100 de compañías de defensa. Infodefensa. September 5. Online: https://www.infodefensa.com/es/2020/09/05/noticia-indra-vuelve-unica-empresa-espanola-companias-defensa.html

94 Centre Delàs. (2020). La industria de defensa y seguridad de fronteras en Catalunya". Informe Centre Delàs 42. January 2020. Online: http://centredelas.org/wp-content/uploads/2020/06/informe42_IndustriaMilitarYSeguridadCatalun%CC%83a_CAST_web_DEF_compressed.pdf

95 Elecnor Deimos (2018). Adjudicado a Elecnor-Deimos, en consorcio con IECISA, el contrato de mantenimiento del Sistema Integrado de Vigilancia Exterior (SIVE). November 7.
Online: https://elecnor-deimos.com/es/mantenimiento-y-mejora-del-sive/

it also has the port of Calais among its clients[96]. Port of Calais is one of the most securitized European port. It is also the port where the majority of violations of the rights of migrants and potential asylum seekers have been reported. ICTS also collaborated with the Israeli technology start-up Virusight[97] to develop a rapid detection system for Covid-19 for the busiest airports. A few days before the announcement of the new application, the media stated that Israel "obstructed" the entry of 100,000 COVID-19 testing swabs that intended for the West Bank[98].

Axis Communications, a supplier of security cameras in the Port of Barcelona, has also participated in the fortification of the Port of Calais, through the installation of 120 surveillance cameras, 20 thermal activity detection cameras and protection and access control devices[99].

The ports of Barcelona and Tarragona are, in turn, a gateway for the export of defense material and armaments, as already indicated by the Centre Delàs d'Estudis per la Pau in 2017[100]. Between 2014 and 2016, around 25% of all the materials classified as "arms, munitions and their parts and accessories" that left from Spain were exported through Catalan port[101]. The destinations were countries that actively participate in conflicts that generate refugees. Besides, Maxam, an explosives manufacturer and one of the largest defense companies in Spain, has close ties with the Port of Tarragona[102], through which it exports the nitric acid produced in the plant of its subsidiary Nitricomax in La Canonja, very close to the port. Nitricomax produces nitric acid, a basic raw material used for the production of explosives and fertilizers.

96 See:: http://www.ictseurope.com/about/our-clients

97 ICTS Europe (2020). Israeli start-up "Virusight Diagnostic" Signs Strategic LOI with ICTS Europe for COVID-19 Rapid Screening in International Airports around the globe. ICTS Europe. September 29. Online: http://ictseurope.com/media/news-pr/israeli-start-up-virusight-diagnostic-signs-strategic-loi-with-icts-europe-for-covid-19-rapid-screening-in-international-airports-around-the-globe

98 Patel, Y. (2020). Palestinians face constant COVID-19 testing shortage. Mondoweiss, September 20. Online: https://mondoweiss.net/2020/09/palestinians-faces-consistent-testing-kit-shortages-during-covid-19/

99 See: https://www.acic.eu/wp-content/uploads/2020/05/etude-de-cas-port-de-calais.pdf

100 Ortega, P. (2017). ¿Armas catalanas?. ElDiario.es, September 8. Online: https://www.eldiario.es/catalunya/adios-a-las-armas/manifestacion-cataluna-armas_132_3203492.html

101 Águila Barbero, P. (2017). Las empresas catalanas, las segundas de España que más armas exportan. El Economista, August 30. El Economista. Online: https://www.eleconomista.es/espana/noticias/8578904/08/17/Las-empresas-catalanas-las-segundas-de-Espana-que-mas-armas-exportan.html

102 Interempresas. 2013. Maxam compra una planta de Acido Nitrico en Tarragona. August 5. Online: https://www.interempresas.net/ObrasPublicas/Articulos/140838-maxam-compra-una-planta-de-acido-nitrico-en-tarragona.html

ENCO

EUROPEAN NETWORK OF
CORPORATE OBSERVATORIES