Revija za kriminalistiko in kriminologijo / Ljubljana 66 / 2015 / 4, 279–290

Security Challenges in the Port of Koper: the Status Quo and Recommendations

Yarin Eski,[1] Boris Kankaraš[2]

The Port of Koper (Luka Koper) is a vital transport hub for Central and Southeast Europe. This paper shall provide a closer look at the Port of Koper and its security. First, a historical overview and the geo-economic ambitions of the port are presented, followed by a concise review of the International Ship and Port Facility Security (ISPS) Code; the Port of Koper, like most global sea ports around the world, must comply with the ISPS Code. The Port of Koper's security governance will then be explored. Finally, an ethnographic study on port security in the Port of Rotterdam (Eski, 2015) shall be discussed, leading to key recommendations for the Port of Koper in advancing its security. The Port of Koper aims to make security services responsible for specific port security tasks, through which multi-agency policing of the port is established, and by applying security technologies more intensively. The recommendations will point out that the Port of Koper must be aware of specific multi-agency policing-related challenges and how "the human element" might react to an increase in security technologies.

Key words: port security, Luka Koper, Port of Rotterdam, multi-agency policing, technologization

UDC: 005.934:627.21

1 Introduction

What happened on 9/11/01 changed our everyday lives everywhere. City centres, malls, traffic infrastructures, but also the global transport network, have been altered significantly by post-9/11 security governance (Simon, 2007). Whilst the consequences for the aviation sector have been well documented (Blalock, Kadivali, & Simon, 2007; Lyon, 2006; Seidenstat, 2004) the drastic changes in post-9/11 security governance structures in maritime transport have been subject to much more limited scrutiny (Eski, 2011). Maritime transport is responsible for moving 80% of everything we consume (UNCTAD, 2015). Ships and ports are essential for the global trade in goods; their importance becomes in particular to everyone's attention as soon as there is a disruption in the flow of goods, which causes prices to increase in supermarkets or at your local gas station. The domain of the maritime world, the mass of people involved and the activities undertaken are significant, if not vital to today's global economy. To safeguard the globalised society's economic growth from danger and insecurities, the maritime domain demands intensive security awareness. Its people and their activities should be protected by establishing high levels of maritime security (Christopher, 2009), in a just way and customised to the maritime sector's specific needs.

In a post 9/11 climate, heightened port security measures are characterised by sophisticated networks of multi-agency policing bodies as different state administered policing and customs organisations operate alongside security services (Urciuoli, Sternberg, & Ekwall, 2010; Hoogenboom, 2010). On the one hand, these agencies and services are considered to deal with the ordinary and mundane aspects of everyday transport; on the other, ports are considered key intersections of crime and control, harm and protection, and threat and security (Chalk, 2008).

In addition to a general lack of public interest in the port as a vital economic site, sociological and criminological interests in ports has been remarkably scarce as well. Criminology in particular has been slow to develop empirical and theoretical research on (trans)port security (Zedner, 2007). So far, and not until recently, only a few criminologists have undertaken long-term research focusing on port security—in particular port security *governance*—in Australia and the USA, the Netherlands, Germany and the United Kingdom (Brewer, 2014; Eski, 2012, 2015; Eski & Carpenter, 2013; Hoogenboom, 2010; Malcolm, 2011). More criminological attention should be paid to port security in other parts of the world too, as well as that criminological light should be shed on security of ports that are *not* listed as the busiest and largest ports, per se.

[1] Yarin Eski, Ph.D., Senior lecturer in Criminology, Liverpool Centre for Advanced Policing Studies, Liverpool John Moores University, United Kingdom. E-mail: y.eski@ljmu.ac.uk

[2] Boris Kankaraš, M.Sc., Port Security Manager, Luka Koper (Port of Koper), Slovenia. E-mail: boris.kankaras@luka-kp.si

When focusing on the 20 busiest ports in the world of the last four years, (only) three European ports are included: Rotterdam (11th), Hamburg (15th) and Antwerp (17th) (UNCTAD, 2014: 66). Central and Southeast European ports are absent, and when looking at the top 20 European ports, Hamburg (2nd), Bremerhaven (4th) and Gdansk (20th) are the most important Central European ports (Port of Rotterdam Authority, 2015). However, there is no port in or close to Southeast Europe listed. These top 20 lists are based on the cargo and container through-put, and not on maritime and port security as a factor. However, seen from a security perspective, Central and Southeast European ports do matter because: "[t]he littorals that surround the Balkan Peninsula are especially prone to abuses, including threats to port security, maritime pollution and natural disasters, piracy, illegal fishing, migration, and the illicit trafficking of humans, drugs, and weapons" (Nation, 2013: 207). The border between Central Europe and Southeast Europe is located on Slovenian territory, so the Slovenian Port of Koper, (next to two smaller Slovenian ports, the Port of Izola and Port of Piran) therefore, forms a vital transport hub for not just Central Europe, but also the coastal zone and hinterland of Southeast Europe (Belt, Chapsos, & Samardžić, 2013).

This article focuses on the Port of Koper, its security governance provision, and considers the very unique security challenges faced by those policing the movement of people and goods at this crucial juncture in Eastern Europe. To contextualise contemporary maritime security governance challenges the articles draws upon lessons learned from an ethnographic study on port security in the Port of Rotterdam (Eski, 2015). As a port considered to be the most secure in Europe (Parliament of Canada, 2006), Rotterdam identifies itself with the continuous advancement of port security: "Rotterdam should be known as the city with the most modern, the cleanest and *most secure port in the world*" (Rotterdam Municipality, 2013: 9 – emphasis added by authors). The discussion will draw on the experience of Rotterdam, the largest port in Europe, to distil learning and best practice development for Koper to engage in developing its port security strategy. First, however, an overview of the Port of Koper shall follow.

2 An overview of the Port of Koper

In 1957, the dredging of the sea bottom on the north coast of the City of Koper ushered in the development of the Port of Koper (Luka Koper in Slovenian language), with the first ship mooring some eighteen months later. Following the development of berths, in 1963 the customs zone was set up. Four years later, the construction of the 31 kilometres railway track from Koper to Prešnica was completed, which enabled the Port of Koper to be included in the European railway system (Jakomin, 2007). One year later, a petroleum facility commenced its activities, followed by the instalment and running of a chemical facility in 1972; that same year a timber facility started to handle cargo. In 1973, the first containers arrived, making the Port of Koper inter-modal and prepared to deal with combined transport, which consequently led to the first container line in Koper connecting with the Mediterranean and to the construction of a container terminal that started to operate in 1979. Six years later, in 1984, a terminal for coal and iron ore was completed, followed by the construction of a grain silo. In 1988, a new cotton warehouse and a terminal for borates and phosphorus acid were constructed, after which oil and alumina terminals were built. With all of these new terminals, towards the end of the 1980s, the cargo throughput rose to 5 million tons (Jakomin, 2007).

The economic and political changes Slovenia experienced in the first half of the 1990s brought new challenges to the country. Due to a significant loss of business, because of retreating Yugoslav customers, the Port of Koper gradually started to deal with customers from Central European markets (Jakomin, 2007). In 1996, the Port of Koper became a public limited company and the company's shares were listed on the Ljubljana Stock Exchange. That year the car terminal began operating and one year later the construction of the Livestock Terminal began. By investing in the separate collection of waste and its processing, setting up sea monitoring, and establishing co-operation with international organizations, the Port of Koper systemically approached environmental management and adapted to the standards of the European Union (Luka Koper, 2015c), for which in 2000 the port received the ISO 14001 environmental certificate.

During 2001 and 2002, investment funds were set aside for the construction of a new shore and the arrangement of moorings and warehousing premises at Pier II. On the initiative of the Ministry of Economy of the Republic of Slovenia, the Port of Koper had a leading role in a pilot project of the Slovenian transport logistic cluster, whose basic objective is the promotion of Slovenian transport routes (Jakomin, 2007). In 2004 the company reorganized the coal and iron ore facility, and renamed it the European Energy Terminal. In the meantime, the cargo throughput exceeded 12 million tons. More importantly, the port received the status of an EU port and border inspection post for goods entering and leaving the EU customs zone, influencing security and border control on a daily basis.

In 2006, a new business strategy was adopted (Luka Koper 2006, 2007), and was still in use in 2015. The company Adria Terminals Ltd. was established in 2007 for the purpose of oper-

ating the inland terminal in Sežana, which enlarged the Port of Koper to an area of 110.000 sq. meters. This was an important step towards the development of the transport logistic centres network, which would in the future provide essential support for the Port of Koper (Luka Koper, 2008). The first part of a new operational and marketing IT system (TinO) was started in the same year; the best ideas in a public competition for a complete port area arrangement were rewarded. The foundation for the extension of the first pier of the container terminal and for the new car warehouse was placed as well in 2007. An important development was the acquisition of the ISO 22000:2005 Food Safety System Certificate, allowing for more types of food-specific cargo handling (Luka Koper, 2008). In 2008, the Port of Koper and the Republic of Slovenia signed a concession agreement, which settled issues related to port activities, management, development and ordinary maintenance of the port infrastructure (Luka Koper, 2009). That same year was also denoted for an extensive investment cycle in the port infrastructure, consisting of an extension of operations on shore of Pier 1 and the building of a new warehouse for 2.750 cars. Noteworthy is the fact that the daughter company Adria Transport Ltd. purchased three train locomotives that started to operate as the first private railroad operation in Slovenia. Its activities are currently oriented towards the Slovenian, Austrian and German markets. 2008 marked the development of consensus between employees and management and a new collective agreement, which invigorates a long-run balance between economic, social and environment viewpoints of development orientations, was formalized (ibid.). The following year, major investments in the infrastructure were made to service modern container ships and other types of cargo (Luka Koper, 2010a). The extended container quay, the enlarged warehousing area, and four new post-Panamax cranes and other equipment, made it possible to receive ships with a capacity up to 8,000 TEU. The construction of a warehouse for cars with 4,100 parking spaces was completed and the construction of a terminal for alcohol was placed into service in 2010 (Luka Koper, 2011a). That same year, a record throughput at Port of Koper's Container Terminal surpassed 400,000 TEU, making it the largest in the Northern Adriatic. Also, a new container service started to provide a direct link between Koper and the Far East. In addition to joining the EU's Eco-Management and Audit Scheme (EMAS), the Port of Koper began providing public information on sustainable development via its website *Living with the Port* (www.zivetispristaniscem.si). This portal provides real-time data on the average hourly noise level, monitored at two peripheral points within the port zone (Luka Koper, 2010b). The European Commission issued a decision as to its co-funding the second stage of the renewal and modernisation of the Koper – Divača railway line, which allowed the Port of Koper to increase rail cargo services to its European hinterland.

Since 2011, more than 100,000 cruise guests passed through Koper's passenger terminal in its first six years of operation. The Slovenian government endorsed the National Spatial Plan (NSP) for the comprehensive spatial arrangement of the Port of Koper, which is a document that will enable the long-term development of the port as well as enhance its competitive advantages (Luka Koper, 2012a, 2012b). In 2012, the Port of Koper commenced dredging the access channels to Basin I - an important step towards enhancing the competitiveness of the port. A container vessel, the 318-metre long and 43-metre wide Mærsk Karlskrona with its 7,908-TEU capacity, and a cruise liner, the Celebrity Silhouette, have been the largest vessels to call at the Port of Koper Luka Koper d.d (Luka Koper, 2013a, 2013b). In fulfilling its societal responsibilities, the Port of Koper commenced publication of data on sea quality via its Living with the Port sustainable development portal (Luka Koper, 2015a). In 2013, the Port of Koper managed to acquire all necessary consents and permits for the creation of sites to deposit dredged silts; this allowed seabed dredging to commence in Basin I to a depth of 13 metres at the Container Terminal quayside (Luka Koper, 2014). The Slovenian Maritime Administration issued a permit to increase permitted maximum draughts of vessels using the Terminal from 11.4 to 12.5 metres, and, as a consequence, container ships calling at the port were able to carry an additional 3,600 TEU. In tandem with these dredging operations, work started on the construction of new container storage facilities at the head of Pier I. In terms of environmental awareness, the Port of Koper has been awarded the European Sea Ports Organization (ESPO) Award in recognition of its work in creating a sustainable future for the port and its surroundings (ESPO, 2015). The ISCC EU certificate has been obtained as well, making it possible for the Port to unload and store oil, rapeseed, soya oil, palm biodiesel, bioethanol and used cooking oil, in accordance with the European Commission (EC) Directive on stimulating the use of renewable energy resources (Luka Koper, 2014).

Today the Port of Koper is a modern multipurpose seaport, and IMO-classified as a mid-size port. It is also an EU port of entry, with full border inspection port facilities. The Port of Koper is a public limited company and Slovenia's sole seaport and maritime gateway to the countries of Central and Eastern Europe (Luka Koper, 2015a). The Port of Koper has a port authority with limitations related to state administration, and port activities and terminal operations are supplemented and enriched by a variety of ancillary services provided by the port's subsidiary enterprises, and further enhanced by the company's provision of logistics and related value-added business services to its clientele (Luka Koper, 2015c). Port operations at Koper are conducted within the context of 12 specialized terminal operations, handling and warehousing various

types of goods, such as container freight, fruit and perishable goods, livestock, cars, timber, as well as dry-bulk, liquid and general cargo (Luka Koper, 2015a). Koper is especially well-connected with the Far East and South-East Asia, with weekly container services with highly competitive transit times.

The Port of Koper's vision is to become a leading port and logistics system provider for the countries in Central and Eastern Europe. Key development directions over the coming years shall encompass the full utilisation of the existing infrastructure and the development of new capacities, particularly in regards to the container freight and car businesses (Luka Koper, 2015a). An upgraded and enhanced service structure shall be created through active marketing and the necessary provision of fully integrated logistics services, together with a variety of supplementary services intended to increase the value of shipped cargos as well as ensure merchandise is market ready (Luka Koper, 2015c). In short, investments shall increase the efficiency and competitiveness of port operations and, at the same time, ensure client satisfaction, reduce energy consumption and maintain ecological standards. In order to understand how these investments and changes to the Port of Koper relate to port security challenges and ambitions, it is vital to explore how port security has developed since the beginning of the 21st century. The following section elaborates the most important piece of international legislation of port security: the International Ship and Port Facility (ISPS) Code.

3 The ISPS Code

Until recently, port security has not been a topic of concern for (international) maritime law and legislation. Instead, the main focus was on ship and cargo safety, of which the most important landmark was the installation of the International Maritime Organization (IMO) and the 1974 International Convention for the Safety of Life at Sea (SOLAS). It took almost 40 years and the events of 9/11 before port security was set high on the agenda. Designed by the IMO, the International Ship and Port Facility Security (ISPS) Code was created after the Twin Tower attacks. It is typical post-9/11 antiterrorist legislation (Eski, 2011), reflected in the Code's preamble:

Following the tragic events of 11th September 2001, the twenty-second session of the Assembly of the International Maritime Organization (the Organization), in November 2001, unanimously agreed to the development of new measures relating to the security of ships and of port facilities for adoption by a Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 (known as the diplomatic Conference on Maritime Security) in December 2002 (ISPS code 2003: 2) (IMO, 2003).

The Code's purpose is to harmonise and standardise port security on a national level, which has rearranged the entire maritime sector (George & Whatford, 2007). The Code was adopted in 2002, pushing ports that accepted the Code to live up to the Code's demands from 1 July 2004 onwards. Compliance with the Code consists of meeting the requirements of its provisions given in the obligatory part A, as well as in non-obligatory part B (IMO, 2003). Although aiming for international integration, harmonisation and standardisation, the Code recognises 'that the extent to which the guidance applies may vary depending on the nature of the port facility and of the ship, its trade and/or cargo' (IMO, 2003: preamble section 9).

The ISPS Code defines several parties and activities to strengthen port security. The Contracting Government (CG) is the principal actor that delegates the roles, as described by the ISPS Code, to organisations and individuals, such as law enforcement, security services and port facilitators. It remains, however, in charge of crucial ISPS Code-based governance of a port. An important CG task is setting the security levels by which a port operates. The measures that come forward should cause minimum interference to daily activities and the flow of transport (section 14.1). There are three levels, where Level 1 is always present, Level 2 stands for heightened security (e.g. significant terrorist threat), and Level 3 is exceptional (e.g. terrorist attack). The CG also approves a Port Facility Security Assessment (PFSA) and a Port Facility Security Plan (PFSP). The PFSA and PFSP must guarantee continuous development and upgrading of security by identifying (threats to) critical infrastructures and weaknesses. Given the differences in security threats and risks per port, PFSP's and PFSA's differ from port to port. Other CG tasks include the monitoring through Port State Control (PSC) and appointing Port Facility Security Officers (PFSOs), and it is up to the PFSO to develop, implement, revise and maintain the PFSP, and to regularly engage with Company Security Officers (CSO). The PFSO also controls one or more port facilities, carries out frequent security inspections, provides adequate personnel training, communicates with authorities about security threats, and appoints security services. Finally, the PFSO cooperates with Ship Security Officers (SSOs) through the design and application of the Declaration of Security (DoS), which is a document that assesses the potential threat ships can pose to a port area and addresses security requirements shared between a port and a ship.

All in all, the ISPS Code outlines how ship and port security ought to be established by a multi-agency of security services, law enforcement and port authorities, overseen by state control (Urciuoli, Sternberg, & Ekwall 2010). The ISPS Code has been introduced and implemented in the Port of

Koper as well; a port that has its global as well as local security challenges to deal with. The following section explores the key challenges the port security department of the Port of Koper is confronted with.

4 The Port of Koper's Security Challenges

The Port of Koper is part of a global transport network, a well-used and serviced port that is a crucial feature of the Slovenian transport and trading infrastructures. The port security challenges that present themselves are many and have changed since the end of the cold war, especially within the last decade. EU and NATO membership has put Slovenia on the world map, and although it remains a relatively small country, the threats of terrorism, cybercrime, climate changes and pollution are just a few of the risks that have the potential to seriously affect the Port of Koper (Kankaraš, 2011; Nation, 2013). The port accommodates all types of industrial facilities where transport and storage of hazardous materials takes place, and these and other kind of highly flammable materials must be protected by fire safety measures. In the Port of Koper, there is also heavy road and railway traffic and a significant amount of heavy transport equipment, which invites all sorts of safety and security-related complexities (Kankaraš, 2011). The fact that the Port of Koper is widely open at the seaside, also brings all kinds of surveillance capacity complexities into play. Currently, the security measures on the landside (the piers) are tightened and security is present on a daily basis (Luka Koper, 2011b). As the Port is in direct connection with the town of Koper, the passenger terminal and general cargo warehouses are separated from the city by a fence, so some of the port (security) operations affect the local community when it comes to their movement and mobility.

In order to guarantee the Port of Koper and its surrounding urban areas remain safe from harm and insecure situations, port security is delivered by the Port of Koper's own security department. The department consists of five subdivisions: a security service unit, a firefighter unit, a crisis management division, a maritime security, and a sensitive data protection unit (Luka Koper, 2015b). For the coordination of cargo handling activities and navigation, a security communication centre is in place. Together these units are responsible for the maintenance of a safe and secure working environment in the Koper docks. The main task of the department is to protect people and property from any risk, in close cooperation with many stakeholders responsible for national security, the port company itself and its business partners (Kankaraš, 2011). The maintenance of security in the Port of Koper demands fast and prudent decisions that will not affect port operations nor decrease security levels. Having a well-trained and professional security staff in place is an important aspect of the department. Furthermore, security awareness of all employees and partners is provided through different types of education, training and (digital) communication (Kankaraš, 2011).

One of the crucial tasks of the port security department is the design and advancement of the Port Facility Security Plan (PFSP) that must be in compliance with the ISPS Code, European directives and Slovenian regulations on ship and port security (Kankaraš, 2013). In order to be compliant, the department has ensured that various security services and equipment are present at the Port of Koper, such as CCTV monitoring, (automated) access control, and different alerting sensors to support and maintain security.

The department's staff is trained and equipped to act as a first responder team in case of an emergency (e.g. fire, explosion, leakage and pollution). The Port of Koper has different emergency plans, business continuity plans, and risk management plans to make sure the right protocols are followed in the case of an emergency. The crisis management centre, along with its staff, is responsible for handling all kinds of emergency scenarios (Luka Koper, 2015b). To safeguard their effective response, the staff undergo regular exercises, in addition to rehearsals that are conducted amongst them, as well as that safety equipment is updated frequently.

As a final note, next to living up to (inter)national maritime and port security regulations, and having various security technologies and services in place, the port security department has established close cooperation with different ministries, the police, customs agencies, security services and the Municipality of Koper (Kankaraš, 2015). This multi-agency policing approach to port security by the department is one of being proactive in maintaining existing and establishing new public-private partnerships (PPPs), because effective multi-agency cooperation and coordination is essential for port security, accompanied by all types of multi-agency policing challenges.

The ambition of the security department is to tackle the increasingly more complex, dynamic and challenging security environment by establishing and organizing an effective corporate security system that will assure proactive and efficient safety and security in and for the Port of Koper (Luka Port, 2013a). A corporate security system could be developed to achieve a more efficient and coordinated approach towards effective port security, and in doing so, security has to be governed from a centralized point of reference. Ideally, at top management levels, various experts are made responsible for management of (decentralized and) independent services, and in this way, smaller teams of experts will communicate

to a core group of expert superiors that is responsible for the overall security governance. For the Port of Koper, such an introduction of centralized, and intensified coordination and cooperation would provide several advantages to run port security more effectively. Currently, management training is in place, during which company specific businesses, risks and organizational structures are taken into account. The development of such a corporate security system requires more co-operation with security services, and it is equally important to (re)consider and advance security technologies to keep up with the dynamics of the Port of Koper's development and changing security challenges. A well trained, professional security staff is fundamental to guarantee the effectiveness of the corporate security system.

In order to understand multi-agency port policing, and the application of a corporate security system consisting of professional(ized) staff and advanced technologies in the port, a study dealing with operational port security realities conducted in the Port of Rotterdam will be considered. Attention shall be paid to the operational realities and attitudes. Particular focus shall be put on 1) how these officers consider multi-agency cooperation and 2) technologization of their daily port security realities. The main findings on these aspects, derived from the study, will be used to provide recommendations for the Port of Koper.

5 Lessons Learned from the Port of Rotterdam

5.1 The Port of Rotterdam

Being a classical European port having roots in medieval times, the Port of Rotterdam grew significantly when the shipping container was introduced and radically changed cargo sizes, ships and worker communities in ports and on deck. The Flag of Convenience (FOC) system changed the entire shipping industry, including the ports of Rotterdam and Koper and is a system that allows a ship to bear a flag of a more fiscally convenient country. It entails the 'flagging out' because of registration at low costs, almost no taxes to be paid, and much freedom on the ship owner's side to employ cheap labour (McConnell, 2012). These major changes in shipping introduced Rotterdam to more shippers coming from an increasing number of places from all over the world. At that same time, technological advancements in ports improved the handling of cargo, which lowered costs (Branch, 2007), and now, due to the technological specialisation and sophistication, there are fully automated berths in Rotterdam, where unmanned vehicles are operated entirely by computer to transport cargo (Van Hooydonk, 2006).

Until 2002, the Port of Rotterdam was the largest and busiest port in the world, and the most important European port. The city centre of Rotterdam used to be directly connected with the port, geographically and socio-economically, but due to the expansion towards the North Sea, the urban community has become increasingly disconnected from the port (Van Hooydonk, 2006). Nevertheless, despite the expansion towards the North Sea and less port business activity in the old city centre harbours, the Port of Rotterdam devotes…

…attention to the relationship between the city and the port. Through various projects, we [PRA] are making the port visible in the centre of Rotterdam. These include the LED screen with images of the port in the entrance hall of Rotterdam Central Station (Port of Rotterdam Authority, 2013: 2).

The recent extension of the port, called the Maasvlakte 2, is directly located at the North Sea, and has the capacity to receive the world's largest cargo vessels. The Port of Rotterdam, from city to shore, is over 40km long with 65 kilometres of quayside, and it covers approximately 12,500ha of land and water, of which 6,000ha consists of business sites and (Port of Rotterdam Authority, 2015).

In all its aspects, the port is an infrastructural node, globally connected and accessible 24/7 to ships that have their first and/or last port of call in Europe. The port is multimodal, meaning trains, inland ships, road transport, and (oil) pipelines come in and out, day and night as well (Van Sluis, Marks, Gilleir, & Easton, 2012). Moreover, because of its size and business, the port is vital to the regional and national economy, contributing 3.5% to the Dutch GDP and providing 180,000 jobs (Port of Rotterdam Authority, 2015). Although the global financial crisis and austerity had a major impact on the maritime transport, the Port of Rotterdam seemed unaffected and handled almost 50% of the world's container port throughput in 2012 (EuroStat, 2012).

5.2 A Study of Operational Realities and Attitudes

The research findings reported on here were generated through ethnographic fieldwork generated in Rotterdam on a project that ran from 2010 until 2015 (Eski, 2015). During fieldwork, that took place from March 2011 until August 2012, port police officers, customs officers and security officers were accompanied and their daily work lives in their familiar work environments were documented by walking along, driving along, sailing along and doing office work. A close-up, ethnographic account was made thus possible by literally being positioned within the port facility perimeters, in port police stations and security companies, and in patrol cars and on ships. The ethnographic methods consisted of

doing interviews, participant observations and at-a-distance observations of 31 security officers, 30 port police officers and 10 customs officers. They executed water- and landside patrols, emergency responses, port traffic control, inspections at port facilities, containers and on-board ships, and preventing and investigating cases of drugs transport, theft, environmental crime and terrorism. Some of these inspections were ISPS Code related, such as Port State Control (PSC) inspections, while other tasks involved establishing a Declaration of Security (DoS) or doing CCTV monitoring of the port facility perimeters. Registration of visitors, truckers and ship crews was also an important task of mostly security officers, and these daily tasks were documented and compiled into one document of raw material (over 2000 pages) and thematically analysed.

5.3 Key Findings on Multi-Agency Port Policing and Port Security Technologization

5.3.1 Multi-agency Partnership or Rivalry

Since the ISPS Code came into force in compliant ports in 2004, and due to other crucial port and maritime security laws, port police, security services and customs agencies started to cooperate (more closely) in Rotterdam (Hoogenboom, 2010). This cooperation is referred to as multi-agency policing through public-private partnerships (PPPs) (Duijnhoven, 2010; Perkins et al., 2007), and is a day to day reality for the participants. One participant, working in the security sector, explained that security services only care about money and not about the public interest of and in the port. Public authorities have "cleaner" goals, he argued, namely that of enforcing law and safeguarding the port. This ambivalent character of the public-private multi-agency in the port leaves behind biases towards each other, preventing or at least slowing doing smooth cooperation, and in extreme situations, these biases stimulate multi-agency conflict instead of cooperation.

A significant issue of conflict for security officers is their desire to receive more information from port police officers and the customs agency, which they do not readily receive. While security officers, they argue, do provide significant amounts of intelligence to port police and customs, this is without receiving any feedback, let alone sensitive, protected information. Security officers, and the few security managers interviewed, realise and agree that the limited information they receive from law enforcement in the port results from legal restraints on the port police and customs officers to share with private parties, such as the security services. This leads to an asymmetrical relationship within multi-agency policing of the port nevertheless:

The moment you try [to receive information] from the police, well, then politics enter. Rules come into play, and then walls are built. […] The police thinks: 'This is police property and is therefore NOT yours' or vice versa. […] We're all doing our thing, whether it is customs, port police, or security services, almost no interaction takes place there … we all have our own little systems, our own sources, all of our stuff that's coming in (Security manager, personal communication).

This specific conflict of port security intelligence interests, in relation to one's information position and between the private security industry and public authorities, is therefore a familiar one. Initiatives to stimulate more information sharing between different policing organizations of the port policing multi-agency, for example, could lead to conflict between those organizations.

On the security officers' side—and also on the port police and customs officers' side—there is suspicion about other multi-agency parties not willing to cooperate and there are negative stereotypes about each other. In the security officers' case, suspicion and negative stereotyping emerges from their having less authority than port police and customs officers. In particular, they assert that the power to arrest is what makes the difference between a security officer and a police officer, and it leads to a low(er) self-image of one's own occupational role in securing the port:

We just need [the port police]. In turn, they [need] us less though, because to them we don't really matter (Security officer 1, personal communication).

There were security officers who deeply despised police officers:

There are cops here… we… don't like each other. I hate those cops. […] Don't want to do anything with any of them. […] But we do make more money than [them]! (Security officer 2, personal communication).

In should be noted that in the above quote regarding a better wage than police officers, the participant feels better about his own line of work in port security. Still, dislike and distrust among each other at the operational level remains prevalent, leading to frustration on the job, perhaps not all the time, but it does play a role on a daily basis when port security is being established. It slows down communication and responses to emergency situations, which can have severe effects on the overall safety and security in a port. Another dimension relevant for the Port of Koper security department to learn from are the attitudes of frontline security officers regarding (the application of) security technologies.

5.3.2 Technologization of Port Security

The ISPS Code and EU directives have led to increasing technological developments in the ports, according to security officers, who were however, cynical about having to work with more surveillance and registration systems. Their attitudes reflect a fear of technology in their worker realities:

Before you didn't have that, each company had its own security guard or security services, right? But nowadays, they [port terminals] only do it [hiring security officers] when it's absolutely necessary, and they invest in expensive alarm systems, you know? […] I remember how you would sit there with three people, at night two people at the minimum. Now you're alone [at night]. Back then though you had one little camera directed at the gate. Now we have 55 cameras. […] The moment there's something wrong somewhere, that camera will directly go to it! You attend to it, and most of times it's a little bird, and when you see trouble, yeah, you call 112. We are not allowed to even go there! (Security officer 3, personal communication).

The concluding sentence above especially reflects how this participant experienced limitations in his job, as he is not allowed to take any action even though he observed an insecure situation. He had to wait passively in the security lodge. Of course, this means a safer way of securing the terminal for him and his colleagues, but nevertheless, for him it meant not being allowed to exercise his job to the fullest extent. In the day to day experience, therefore, security officers can experience how technology pacifies the worker, and in the mind of the security officer, remaining passive increases the possibility for an insecure situation to remain unresolved or to get worse.

Many more security officers felt pacified by technology, and they are worried that their job position is threatened by technological solutions, which is a recurring complexity of technologization (Adam & Allan, 2014; Smith, 1989). They can be replaced by technology, and even if they keep their job, the nature of the job changes, it was argued. Participants would explain that it requires the right people for handling such systems, preferably people with the right knowledge and educational background:

It's about the equipment AND people, because people you employ, they should be able to work with it of course, but they should have the obligated papers [e.g. certificates] (Security officer 4, personal communication).

Thus, if new technological advancements are to work, operational officers must perceive the operating of security and surveillance systems to be undertaken by well-educated staff, to which they do think they do not belong. The more complex a technological application becomes and has an actual positive effect on security, the more participants expect operators to be better educated. Otherwise, such technologies are not expected to have any significant effect at all. The effectiveness of (new) technology, in the eyes of the participants, does not depend on the technology itself, but on the capabilities of the one who has to work with it.

In addition, technology is referred to as a means to obtain a secured situation in the port environment by the participants, but not without the interference of the "human element". Any technology that shuns the idea of being fully operational by itself and still be completely reliable, will not be taken seriously. Such technology therefore influences its own (non-)acceptance within the port security domain and by those responsible for operational port security. On a similar note, the increasing multiplicity and complexity of tasks as a result from having fewer personnel that can operate more systems, leads to errors, security officers explained:

We have to have CCTV camera's, in the system, and we have to look around the territory with those camera's regularly. Well, then you notice, because of the workload, you are not able to do so (Security officer 5, personal communication).

In a nutshell, increasing technologization of port security and surveillance could result in *fewer* people operating *more* systems, which bares the creation of security officers being too busy with not risking to make an error. After all, an error leads to a negative evaluation of one's job performance, as was indicated. Human errors because of handling technologies wrongly, leads to participants experiencing stigmatization, because all their errors on the job are recorded. As much as their own job is to control the security situation in a port with technological solutions, to be (more) controlled *by* technologically advanced registration systems, leads to fears of being stigmatized. They feel they are not allowed to make mistakes, which makes them experience the incapability to live up to the expectations of their superiors, and that frustrates them.

Besides having these frustrations and fears, there is the possible fear of criminogenic effects *because of* technology. Whatever you may undertake in order to control and secure with whatever new technologies there are available, security officers (as well as participants at the port police and customs agencies) believe that their criminal counterpart (e.g. drug trafficker, human traffickers, terrorists) that illegally obtains technologies or advances its own technological supremacy is problematic. The War on Terror brought about much technological development (Ceyhan, 2008), and given the end-users' perceptions of port security technology, it seems the participants are afraid of technological developments made for themselves that could easily be used by a hostile party as well.

Another concern of security officers about the technologization of their daily work is that the purchase of (new) technologies may not always be done so for port security per se:

When you're at a construction site and you use your [thermographic] camera, you can indeed see someone walking. It of course has its function, but sometimes I think you don't use it that often actually. It's a bit of eye-catching for the customers [I secure for]. […] A bit of commercial logic (Security officer 6, personal communication).

The security officer thinks its use is only convenient every so often, and has doubts about the true intention behind the purchase of this technology. In his opinion, his company wants to look like a professional security company by having "shiny boxes" of cutting-edge technological equipment that attracts (new) clients, instead of having sensible solutions for present and relevant insecurities in the port environment.

6 Recommendations for the Port of Koper

The growth of the Port of Koper is continuing, which will lead to more complex, dynamic and challenging security environments in Koper. As mentioned above, the Port of Koper security department management is aware of these changing security challenges and shortages in the security department's capacity to provide effective and reliable security levels. There are solutions available, however, time and money should be invested. What also matters is political decision-making at the national level, because '[t]o address the challenge of maritime security effectively, a paradigm shift is required' (Nation, 2013: 207). Such a shift, requires the Slovenian government to move beyond 'the national domain into a multilateral context, facilitating greater cooperation and interoperability among all regional organizations, states, and agencies with maritime responsibilities. […] [and] coordination in the area of maritime security could serve as an impetus to regional cooperation in South East Europe as a whole' (Nation, 2013). It is then necessary for the Slovenian government to re-evaluate the regulations of the private security sector, in order to enable private security to become more efficient in the port, while releasing port police forces from certain security tasks who in turn can intensify their particular typical police-related tasks, such as investigations. However, seen from an anchored pluralist perspective on security governance (Loader & Walker, 2007), the state still has the duty to make sure port security provided by stakeholders (especially private) is monitored and legally sound.

National critical infrastructures secured by such security services, in accordance with private security sector law, should have high priority for the Port of Koper as well. Slovenia has been privatizing significant amounts of its public tasks to the private sector, such as is the case with the nuclear power plant in Krško which has a special regulation about security as issued by the Ministry of the Interior (Pravilnik o fizičnem varovanju jedrskih objektov, jedrskih in radioaktivnih snovi ter prevozov jedrskih snovi, 2013). Although there are certain efforts toward strengthening private and public (national) security sector cooperation, the improvements are still weak and too slow in relation to national legislation that arranges port and maritime security.

Up-to-date and real time information coming from a wide variety of intelligence sources is essential to maintain security and deter threats. Therefore, exchange of (real time) intelligence is a matter of cooperation between the security services, in particular operational security managers and security officers, and law enforcement, such as the port police and preferably the customs agencies as well. Under the umbrella of dedicated organizations and associations (e.g. the Slovenian Private Security Sector Board, the IMO, the COESS, and the EU), such a network of port security stakeholders could be further developed. Under specific procedures and vetting, the membership to that network can be granted, enabling its members to share and retrieve security intelligence without having to fear one might be breaking the law. Something similar has been attempted for the Port of Rotterdam, where the Seaport Police Rotterdam, Securitas and Trigion agreed to exchange intelligence with each other (RTV Rijnmond, 2011).

The Port of Koper is a domain where it is logical to introduce and develop such information sharing and (further) privatization of port security and delegate tasks to security services. There is much support in the port business community to make the necessary efforts for implementation of solutions that are available (Luka Koper, 2015b). The primary aim is to establish and organize an effective corporate security system that will assure proactive and efficient safety and security in and for the Port of Koper. To efficiently maintain adequate levels of security and respond and handle different incidents, it is necessary to develop the Port of Koper security system on a higher level, keeping in mind the current status of the Port of Koper and its development plans for the future, in which a corporate security system is a must. Security coordination is important between company managers and other stakeholders. The organization of multi-agency communication and coordination demands additional training of dedicated managers in departments that are responsible and authorized for specialised security functions in the department. This is especially important at the operational level. Key advancements that must be made to reach this aim consist of an expansion of security capacity by working together (more closely) with 1) security services who provide security officers and 2) the (re) consideration of (new) technologies to use.

Based on the lessons learned from the study explored in the previous section, it will be crucial for the Port of Koper security department to consider the demanding, and possibly conflictive character of multi-agency policing and delivering port security within a network of multiple public-private partners. It became apparent that there are biases among security officers towards other multi-agency actors, in particular the port police that need to be overcome in order to prevent the disruption of smooth cooperation and potential conflicts. A significant issue for the Port of Koper to avoid, or at least to be kept at a minimum, is security officers' experience in sharing information with public authorities such as the port police. Initiatives to share more information with each other should not lead to its contradictory consequence, which is an unwillingness to share information. Moreover, it is as important to get rid of suspicion regarding the other multi-agency parties and prevent negative stereotyping of each other. In particular, security officers could again experience inequality because of having less authority than the port police. This needs to be exposed, discussed and agreed on among all relevant parties. Authority jealousy, suspicion and negative stereotyping can lead to frustration on the job, and could eventually lead to miscommunication and slow(er) responses to emergency situations. Altogether it could have severe effects on the overall safety and security of the Port of Koper, and therefore of the maritime transport in Central and Southeast Europe.

Another prominent recommendation for the Port of Koper, based on this study, is to be aware of concerns of security officers about (further) technologization within the port security domain. It became clear that the security officers in Rotterdam were cynical about the application of additional port security technologies. They even fear the dehumanizing and pacifying effects of technology in their daily tasks to secure the port. Port security (technological) innovation in the Port of Koper should never lead to creation of such fears and insecurity, because it can, like multi-agency conflict and miscommunication, increase the chances that an insecure situation remains unresolved or becomes worse. Participants have additional worries about not having the right (IT) capabilities and capacities to work with (new) systems and technologies, which could lead to non-acceptance of security systems as well. Whereas, they should actually improve their work and therefore the overall port security situation. The Port of Koper security department therefore needs to make serious efforts in training security officers in handling IT-systems and technologies they are unfamiliar with, otherwise, the installation of the planned corporate security system may have no effect whatsoever on port security in Koper. Perhaps even an opposite effect. It is also essential to open up the debate about not having to fear a partial if not complete take-over of hands-on security work by technology. The human element should remain present in providing port security and therefore there should be an acceptable space to make errors. This is a risk that is inherently part of providing port security, if one wants to keep the human factor. Henceforth, it is crucial for the Port of Koper to establish trust among security staff in novel security technologies, while making sure that the security officers, who literally are the human element, are not replaced.

Finally, and not immediately coming forward from this study's results but rather from the fact the study *was* undertaken in the port security domain, and conducted from a criminological perspective, it is strongly recommended that the Port of Koper security department makes use of several relevant fields of expertise and experts. Experts in the fields of criminology, security, maritime and port engineering, statistical analysis, and prevention and disaster management are needed to create and critically re-evaluate efficient security systems to benefit the Port of Koper's security, and eventually the flow of transport in and out of Slovenia.

7 Conclusion

In this paper, the authors argue that the Port of Koper is an important port that functions as a vital transport hub for not just Central Europe, but also the coastal zone and hinterland of Southeast Europe. An historical overview of the port was outlined, as well as an indication of the current geo-economic ambitions of the port. This was followed by an explanation of the ISPS Code – the most important legislation for maritime and port security – and which specific threats there are for the Port of Koper, and which organisations are responsible to deal with these and other types of security challenges. More importantly, the port security ambitions of the Port of Koper were described, of which the main aim is to join forces with security services that will become responsible for specific port security tasks in the Port of Koper. In order to have provided the specific recommendations for the Port of Koper to take into account when fulfilling its aim to put a corporate security system in place, the authors discussed an ethnographic study of Port of Rotterdam security officers who fulfil those exact corporate security system-related tasks in Rotterdam. Therefore, the core of this paper consisted of which lessons there can be learned from the Rotterdam study. The two key findings relevant to the recommendations were the attitudes of security officers towards multi-agency policing of the port and their attitudes towards the technologization of their daily work. From these findings, several recommendations were drawn and described in the previous section, and the autors strongly recommend that the Port of Koper takes notice of specific multi-agency cooperation related struggles and challenges, and should be cautious about the application of secu-

rity technologies. It is crucial to be real about multi-agency policing and about the human element in port security (technologies). In conclusion, if the Port of Koper will consider these dimensions seriously, the improvement of its port security is very well possible.

References

1. Adam, B., & Allan, S. (2014). *Theorizing culture: Critique*. Abingdon: Routledge.
2. Belt, D., Chapsos, I., & Samardžić, D. (2013). Maritime security challenges in South-East Europe. In S. Cross, S. Kentera, R. Vukadinovic, & R. C. Nation (Eds.), *Shaping South East Europe's security community for the twenty first century: Trust, partnership, integration*, (pp. 134–150). Basingstoke: Palgrave Macmillan.
3. Blalock, G., Kadiyali, V., & Simon, D. H. (2007). The impact of post-9/11 airport security measures on the demand for air travel. *Journal of Law and Economics, 50*(4), 731–755.
4. Branch, A. E. (2007). *Elements of shipping*. Abingdon: Routledge.
5. Brewer, R. (2014). *Policing the waterfront: Networks, partnerships, and the governance of port security*. Oxford: Oxford University Press.
6. Ceyhan, A. (2008). Technologization of security: Management of uncertainty and risk in the age of biometrics. *Surveillance & Society, 5*(2), 102–123.
7. Chalk, P. (2008). *The maritime dimension of international security: Terrorism, piracy, and challenges for the United States*. Santa Monica, CA: RAND Corporation.
8. Christopher, K. (2009). *Port security management*. Boca Raton: Taylor & Francis Group.
9. Duijhoven, H. L. (2010). *For security reasons narratives about security practices and organizational change in the Dutch and Spanish railway sector*. Amsterdam: VU University Press.
10. Eski, Y. (2011). 'Port of call': Towards a criminology of port security. *Criminology & Criminal Justice: An International Journal*, *11*(5), 415–431.
11. Eski, Y. (2012). Cultures and people of the post 9-11 port securityscape. *International Journal of Criminology & Sociological Theory*, *5*(3), 947–959.
12. Eski, Y. (2015). *The portsecurityscape: an ethnography* (PhD thesis). Glasgow: University of Glasgow.
13. Eski, Y., & Carpenter, A. (2013). Policing in EU seaports: Impact of the ISPS code on port security post-9/11. In M. O'Neill, K. Swinton, & A. Winter (Eds.), *New challenges for the EU internal security strategy* (pp. 71–95). Newcastle upon Tyne: Cambridge Scholars Publishing.
14. European Sea Ports Organisation [ESPO]. (2015). *ESPO award 2014*. Retrieved from http://www.espo.be/index.php?option=com_content&view=article&id=477&Itemid=81
15. EuroStat. (2012). *Top 20 container ports in Europe*. Retrieved from http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/File:Top-20_container_ports_in_2012_-_on_the_basis_of_volume_of_containers_handled_in_(1000_TEUs(1)).png)
16. George, B., & Whatford, N. (2007). Regulation of transport security post-9/11. *Security Journal*, *20*(3), 158–170.
17. Hoogenboom, B. (2010). *Bringing the police back in: Notes on the lost & found character of the police in police studies*. Dordrecht: SMVP.
18. IMO. (2003). *ISPS Code*. London: IMO.
19. Jakomin, L. (2007). *Luka Koper: 50 years – for new horizons*. Koper: Luka Koper.
20. Kankaraš, B. (2011). *Counter-terrorism in the Port of Koper*. Ljubljana: University of Maribor.
21. Kankaraš, B. (2013). *Port security program 2013*. Koper: Port security department.
22. Kankaraš, B. (2015). *Luka Koper d.d., Port security department*. Koper: Slovenian Association for Corporate Security.
23. Loader, I., & Walker, N. (2007). *Civilizing security*. Cambridge: Cambridge University Press.
24. Luka Koper (2006). *Annual report of Luka Koper, d.d. 2005*. Retrieved from http://www.luka-kp.si/eng/annual-reports
25. Luka Koper (2007). *Annual report of Luka Koper, d.d. 2006*. Retrieved from http://www.luka-kp.si/eng/annual-reports
26. Luka Koper (2008). *Annual report of Luka Koper, d.d. 2007*. Retrieved from http://www.luka-kp.si/eng/annual-reports
27. Luka Koper (2009). *Annual report of Luka Koper, d.d. 2008*. Retrieved from http://www.luka-kp.si/eng/annual-reports
28. Luka Koper (2010a). *Annual report of Luka Koper, d.d. 2009*. Retrieved from http://www.luka-kp.si/eng/annual-reports
29. Luka Koper (2010b). *Environmental report of Luka Koper, d.d. 2009*. Retrieved from http://www.zivetispristaniscem.si/index.php?page=static&item=14
30. Luka Koper (2011a). *Annual report of Luka Koper, d.d. 2010*. Retrieved from http://www.luka-kp.si/eng/annual-reports
31. Luka Koper (2011b). *Environmental report of Luka Koper, d.d. 2010*. Retrieved from http://www.zivetispristaniscem.si/index.php?page=static&item=14
32. Luka Koper (2012a). *Annual report of Luka Koper, d.d. 2011*. Retrieved from http://www.luka-kp.si/eng/annual-reports
33. Luka Koper (2012b). *Environmental report of Luka Koper, d.d. 2011*. Retrieved from http://www.zivetispristaniscem.si/index.php?page=static&item=14
34. Luka Koper (2013a). *Annual report of Luka Koper, d.d. 2012*. Retrieved from http://www.luka-kp.si/eng/annual-reports
35. Luka Koper (2013b). *Environmental report of Luka Koper, d.d. 2012*. Retrieved from http://www.zivetispristaniscem.si/index.php?page=static&item=14
36. Luka Koper (2014). *Annual report of Luka Koper, d.d. 2013*. Retrieved from http://www.luka-kp.si/eng/annual-reports
37. Luka Koper (2015a). *Annual report of Luka Koper, d.d.* 2014. Koper. Retrieved from http://www.luka-kp.si/eng/annual-reports
38. Luka Koper (2015b). *Luka Koper handbook: Port security*. Retrieved from http://www.luka-kp.si/eng/port-security
39. Luka Koper (2015c). *The Luka Koper group business strategy until 2030 and the company's and group's strategic business plan 2016 – 2020 (Summary)*. Retrieved from http://www.luka-kp.si/eng/mission-vision-strategy
40. Lyon, D. (2006). Airport screening, surveillance, and social sorting: Canadian responses to 9/11 in context. *Canadian Journal of Criminology and Criminal Justice, 48*(3), 397–411.
41. Malcolm, J. A. (2011). *The securitisation of the United Kingdom's maritime infrastructure during the 'war on terror'* (PhD thesis). Warwick: University of Warwick.
42. McConnell, M. L. (2012). Forging or foregoing the 'Genuine Link'? A reflection on the Maritime labour convention, 2006 and other approaches. In A. Chircop, N. Letalik, T. L. McDorman, & S. Rolston (Eds.), *The Regulation of international shipping: International and comparative perspectives – essays in honor of Edgar Gold* (pp. 401–428). Leiden: Martinus Nijhoff.

43. Nation, R. C. (2013). *Conclusion*. In S. Cross, S. Kentera, R. Vukadinovic, & R. C. Nation (Eds.), *Shaping South East Europe's security community for the twenty first century: Trust, partnership, integration* (pp. 197–216). Basingstoke: Palgrave Macmillan.
44. Parliament of Canada. (2006). *Debates of the senate (Hansard) - 1st Session, 39th Parliament, 143*(28). Retrieved from http://www.parl.gc.ca/Content/Sen/Chamber/391/Debates/028db_2006-06-27-e.htm
45. Perkins, N., Penhale, B., Reid, D., Pinkney, L., Hussein, S., & Manthorpe, J. (2007). Partnership means protection? Perceptions of the effectiveness of multi-agency working and the regulatory framework within adult protection in England and Wales. *Journal of Adult Protection, 9*(3), 9–23.
46. Port of Rotterdam Authority. (2013). *Investing in the future.* Retrieved from http://www.Abridged-Annual-Report-2013-Port-of-Rotterdam-Authority.pdf
47. Port of Rotterdam Authority. (2015). *Top 20 European ports.* Retrieved from https://www.portofrotterdam.com/sites/default/files/Top%2020%20European%20container%20ports.pdf
48. Pravilnik o fizičnem varovanju jedrskih objektov, jedrskih in radioaktivnih snovi ter prevozov jedrskih snovi [Regulation on physical security of nuclear facilities, nuclear and radioactive materials and transportation of radioactive materials]. (2013). *Uradni list RS*, (17/2003).
49. Rotterdam Municipality. (2013). *ROTTERDAM climate proof: The Rotterdam challenge on water and climate adaptation*. Retrieved from http://www.rotterdamclimateinitiative.nl/documents/RCP/English/RCP_folderalgemeen_eng.pdf
50. RTV Rijnmond. (2011). *Zeehavenpolitie trekt op met beveiligingsbedrijven.* Retrieved from http://www.rijnmond.nl/nieuws/23-12-2011/zeehavenpolitie-trekt-op-met-beveiligingsbedrijven
51. Seidenstat, P. (2004). Terrorism, airport security, and the private sector. *Review of Policy Research, 21*(3), 275–291.
52. Simon, J. (2007). *Governing through crime. How the war on crime transformed American democracy and created a culture of fear*. Oxford: Oxford University Press.
53. Smith, M. R. (1989). Technologizing office work. *Society, 26*(4), 65–72.
54. UNCTAD. (2014). *Review of maritime transport 2014*. New York: United Nations.
55. UNCTAD. (2015). *Review of maritime transport 2015*. New York: United Nations.
56. Urciuoli, L., Sternberg, H., & Ekwall, D. (2010). *The effects of security on transport performance.* Paper presented at WCTR congress 11–15 July, 2010. Lisbon, Portugal.
57. Van Hooydonk, E. (2006). *Soft Values of Seaports: a Plea for Soft Values Management by Port Authorities*. Apeldoorn: Garant Publishers.
58. Van Sluis, A., Marks, P., Gilleir, F., & Easton, M. (2012). Nodal security in the ports of Rotterdam and Antwerp. In M. Fenger, & V. Bekkers (Eds.), *Beyond fragmentation and interconnectivity: public governance and the search for connective capacity* (pp. 73–94). Amsterdam: IOS Press.
59. Zedner, L. (2007). Pre-crime and post-criminology? *Theoretical Criminology*, *11*(2), 261–281.

Varnostni izzivi v Luki Koper: status quo in priporočila

Dr. Yarin Eski, predavatelj kriminologije, Liverpool Centre for Advanced Policing Studies, Liverpool John Moores University, United Kingdom. E-pošta: y.eski@ljmu.ac.uk

Mag. Boris Kankaraš, vodja področja pristaniške varnosti, Luka Koper, Slovenija. E-pošta: boris.kankaras@luka-kp.si

Koprsko pristanišče (Luka Koper) predstavlja ključno transportno povezavo za Srednjo in Jugovzhodno Evropo. Prispevek podaja vpogled v pristanišče in njegovo varnost. V uvodu so predstavljeni zgodovina razvoja in geoekonomski cilji pristanišča. Nato se prispevek natančneje osredotoči na Mednarodni zakonik o varnosti ladij in pristanišč (angl. *International Ship and Port Facility Security Code* – ISPS), ki tako kot za večino pristanišč velja tudi za koprsko pristanišče. V nadaljevanju članek obravnava upravljanje z varnostjo, sledi pregled etnografske študije pristaniške varnosti v pristanišču Rotterdam (Eski, 2015) ter priporočila za nadgradnjo varnosti v koprskem pristanišču. Luka Koper želi vzpostaviti varnostni sistem, ki bo vzpostavil takšno organizacijo varnostnih služb, ki bodo pristojne za posamezna specifična varnostna področja in naloge, kar omogoča pluralno policijsko dejavnost in pri tem predvideva tudi intenzivnejšo uporabo sodobnih varnostnotehničnih sistemov. Priporočila izpostavljajo izzive, ki jih je treba upoštevati ob takšni organizaciji varnosti in mogočih reakcijah posameznikov na povečano implementacijo varnostnotehničnih sistemov in tehnologij.

Ključne besede: pristaniška varnost, Luka Koper, pristanišče Rotterdam, pluralna policijska dejavnost, tehnologizacija

UDK: 005.934:627.21