CoESS

Acting as the voice of the **security industry**

Best practices in transport security

Table of Contents

ACI Europe	European Airport Council
AEO	Authorised Economic Operator
ASSA-i	Aviation Security Services Association
AVSEC	Regulatory Committee for Aviation Security
CBRN	Chemical, Biological, Radiological, and Nuclear
CEN	European Committee for Standardisation
CoESS	Confederation of European Security Services
EASA	European Aviation Safety Agency
ETD	Explosives Trace Detection
FBI	Federal Bureau of Investigation
HME	Homemade Explosives
ICT	Information and Communication Technologies
IED	Improvised Explosive Devices
IMO	International Maritime Organisation
ISPS Code	International Ship and Port Facility Security Code
LANDSEC	Expert Committee on Land Transport
MARSEC	Regulatory Committee for Maritime Security
PFSA	Port Facility Security Assessment
PFSO	Port Facility Security Officer
PSC	Private Security Company
SAGAS	Stakeholder Advisory Group on Aviation Security
SAGMAS	Stakeholder Advisory Group on Maritime Security
SOLAS	International Convention for the Safety of Life on Sea
TAPA	Transported Asset Protection Association
TSR	Trucking Security Requirements
UAV	Unmanned Aerial Vehicle
UITP	European Association for Public Transport
UNI Europa	European Services Workers Union
VaaW	Vehicles as a Weapon

About CoESS

The Confederation of European Security Services (CoESS) acts as the voice of the private security industry, covering 19 European Union (EU) Member States and a total of 24 countries across Europe, representing around 2 million licensed guards and 45,000 companies, and generating a turnover of €40M+.

The private security services provide a wide range of services, both for private and public clients, ranging from European Union institutions buildings to nuclear plants, airports, Critical Infrastructure facilities, inter-modal transport hubs, public transport stations and areas, and national governmental agencies and institutions (such as asylum seekers centres, public hospitals, universities, etc.).

Definition of Private Security Companies

As defined in CEN EN 15602 standard on "Security Services Providers – Terminology", "private security company" is one that provides private security services. In this report, the term is used interchangeably with **economic operator**, which is the term used in legislation and standards.

Following the definition in the standard, services provided by security companies are aimed at the protection of people, property and assets. These may include the following services (non-exclusive list):

→ manned guarding – access/exit control, airport security checks, armed security officer/guard, port security checks, reception security, site security, static guarding, store detective;

→ mobile patrolling and mobile site/area patrolling;

→ alarm response – alarms, monitoring and alarm receiving centre, alarm receiving and monitoring centre operator, alarm response, alarm response officer;

→ key holding – key holding and key storage;

→ event security – crowd controller, crowd control supervisor, crowd control management;

→ door security and supervisor;

→ close protection/body guarding;

→ public order services – city patrolling, transport security;

→ etc.

It excludes military services.

Executive Summary

When we talk about security in aviation, maritime, and land transport, we're talking about a sector that is fundamental to European economics, mobility, trade, logistics, and tourism. Whether we travel, trade, or simply go to work in the morning – hundreds of million citizens in the EU heavily rely on safe, secure, and efficient transportation. The role of aviation, maritime, and land transportation in our daily lives and business will only increase, as international networks become more connected in the years to come.

At the same time, means of transportation are Critical Infrastructure that is increasingly vulnerable to intentional unlawful acts against public authorities, businesses, and the public. Criminal networks and terrorist groups have targeted means of transportation for decades. Risks range from attacks with firearms and explosives to illegal trafficking and theft. But, these threats evolve. Criminal networks often adapt their modus operandi to existing security measures. With the persistent terrorist threat originating from ISIS fighters returning from conflict zones in the Middle East, we must also prepare for threat scenarios that include new ways of using explosives, cyberattacks, drones, lone-wolves, or even chemical, biological, nuclear and radiological (CBRN) material.

Therefore, in this report CoESS has developed informal guidelines and best practices for policymakers and security services protecting different types of transport: aviation, maritime, and land. With these guidelines, CoESS intends to contribute to a broader debate around transport security. They shall feed into current policy discussions, and support relevant authorities in developing future policies and updated security measures according to the evolving risk environment.

Attacks on European transportation networks are becoming more frequent, which makes a pro-active, pre-emptive approach towards the implementation of security measures necessary. European legislative frameworks of aviation, maritime, and land transportation, and their implementation vary widely – from the highly regulated aviation transport sector to land transport, where no EU legislation exists. But, they all face very similar threat environments, show comparable loopholes in the security supply chain and can learn from each other.

We do not call for major changes in existing laws and regulations, but for the introduction of more preventive security measures in each transportation mode. It is important to introduce new measures independently from past attacks and based on distinct security risk assessments. Further, we also recognise a significant variation in legislation, standards, and their implementation across the Member States.

Important ways to improve transportation security must also include the introduction of public procurement quality guidelines for the contracting of Private Security Companies (PSC). CoESS therefore promotes the Best Value approach (**www.securebestvalue.org**) to select a security provider.

Further, better cooperation and exchange of information and best practices across the large variety of stakeholders involved in security supply chains and the functioning of transportation hubs is crucial. PSCs can be an important partner in this effort, as they are often first in-line responders to incidents, qualifying them as a valuable source of information and partner in the set-up of security plans. Furthermore, PSCs are not even able to face possible third parties' claim in the event of an incident, which could relate to amounts exceeding available insurance coverage. Here, we need a coherent liability regime.

Last but certainly not least, creating a security culture across stakeholder organisations and, most importantly, among the public is a winning strategy in anticipating both security and safety issues. The more vigilant and informed we are, the better prepared we will be.

Introduction and Background

Today, the transportation sector is crucial to European citizens, economies and the functioning of our society. Entire businesses depend on cargo networks. Cities cannot function without efficient and safe public transportation systems. Travelling with airplanes, ships, and trains lies at the heart of cross-border mobility in Europe. Our transportation networks are highly important Critical Infrastructures and fundamental to national security.

At the same time, the recent series of attacks, especially in land and aviation transportation, shows that the EU is facing threats from terrorists and criminal networks that are willing and capable to kill innocent citizens and severely disturb transportation networks. New technologies that are available to these actors lead to an increasingly evolving threat environment.

With this report, CoESS developed informal guidelines and best practices for policymakers and security services in different types of transport: aviation, maritime, and land. With the provided guidelines, CoESS intends to contribute to a broader debate around transport security. They shall feed into current policy discussions, and support relevant authorities in developing future policies and updated security measures according to the evolving risk environment. Members and chairmen of CoESS expert committees, for example from Guarding and Maritime Security Committees, as well as the Aviation Security Services Association (ASSA-i) contributed to this report.

CoESS will provide an assessment of existing threats to the different modes of transportation, both related to the security of passengers and cargo. We will provide an overview of relevant legislation and standards on EU-level and identify gaps, shortcoming and loopholes in the security supply chain based on our experience. Following an assessment of future developments and threats, we will provide recommendations not only for legislation and the implementation of further security measures, but on the functioning of the security supply chain and cooperation of involved stakeholders as a whole.

Executive Summary

A safe and efficient aviation transportation sector is a crucial pillar of European trade and tourism. Following a number of terrorist incidents over the past 15 years, aviation security in Europe has been subject to strict security legislation and standards.

Still, aviation transportation infrastructures remain vulnerable to a large range of threats including homemade explosives (HMEs); chemical, biological, radiological, and nuclear (CBRN) material; insider threats; cyberattacks; and drones. ISIS fighters returning from conflict regions and the availability of new technologies that circumvent security measures are further driving this threat environment. The 2016 attacks on the Brussels Airport and the rising number of incidents with drones at airports confirm this development.

European legislation has until now been very reactive to such developments. We believe that this should evolve from a responsive to a more pro-active legislative approach to effectively address and anticipate emerging threat scenarios. Additionally,

CoESS and the Aviation Security Services Association – international (ASSA-i) also consider that there is too much room for interpretation in the common basic standards and that gaps remain.

From the standpoint of private security companies (PSCs), gaps also include the lack of specific rules for public procurement, shortcomings in communication and exchange of information among all stakeholders involved in aviation security and the inexistence of a harmonised liability regime for the consequences of terrorist attacks.

Apart from enhanced common security standards in EU legislation, this chapter recommends to select PSCs based on existing norms and standards such as EN 16082:2011[1] and calls for a clear EU initiative to efficiently address the issue of liability for all different sectors concerned. Further, it is key for a functioning security chain at airports to establish efficient communication frameworks for all stakeholders involved in aviation security.

Introduction

Aviation security is an integral part of European trade, tourism, and mobility. In 2016, European airports welcomed 2 billion passengers – a new record[2]. They contributed to the employment of 12.3 million people earning € 356 billion in income in 2015, and generate € 675 billion in GDP each year, equal to 4.1% of GDP of Europe[3].

As the aviation sector grows, it remains very vulnerable to evolving threat environments. The overall objective of the EU's aviation security policy is to protect the people and assets, and more generally European economies from the consequences of unlawful intentional acts against civil aviation and airports.

This chapter will assess current risks to aviation security and provide an overview of existing legislation, standards, their implementation and respective gaps. On this basis we provide recommendations for improvements and further actions from the point of view of private security companies (PSCs).

[1] http://www.assa-i.org/project-and-standards.php?page=en-standard
[2] Eurostat (2015). Air transport statistics. Available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/Air_transport_statistics (retrieved: 25.09.2017)
[3] ACI Europe (2015). Economic Impact of European Airports - A Critical Catalyst to Economic Growth.

The chapter is written in cooperation with ASSA-i, the Aviation Security Services Association – international (For further information about ASSA-i, please refer to www.assa-i.org). ASSA-i is a member of CoESS and brings together the main players in private providers of airport security services.

Risk Assessment

Aviation security is key for trade, mobility, and tourism in Europe. Due to a constantly high risk level, strict security measures have been set in place since the 9/11 attacks in the US. But, the aviation sector remains very vulnerable to security threats. An increasing number of ISIS returnees from the Middle East are clearly committed to conduct attacks on European soil, for instance at airports, and have experience in bomb-making and the handling of arms. New technologies such as cyberattacks and drones provide further possibilities to circumvent airport security. If airport security is deficient, it puts a high risk on aviation security as a whole.

Homemade explosives (HME) and improvised explosive devices (IEDs)

HMEs and IEDs present a constant threat to aviation security. Terrorist networks continue to work on ways to circumvent security measures – from explosive liquids hidden in underwear to bombs stowed in laptops. Targets include both airplanes and public spaces at airports and terrorists are still too often successful in implementing their plans.

The bombings at Brussels Airport in 2016 show that the risk of attacks on areas of landside airport infrastructure is high. It resulted in 11 casualties and 81 people were injured. The airport stayed closed for almost two weeks and it took months before it went back to being fully operational.

The explosion on-board the EgyptAir flight from Cairo to Saint Petersburg in 2015 and the infamous underwear-bomber in the Northwest Airlines flight from Amsterdam to Detroit in 2009 show that aircrafts also remain popular targets for IED attacks. Many of these incidents were followed by tightened security measures and legislation.

The United State government's ban on laptops, currently applicable to airports in the Middle East, shows that legislation is in a constant struggle to stay ahead of evolving tactics of terrorist networks. Legislation therefore needs to adequately address the risk of attacks with IEDs concealed in cabin and hold baggage.

Chemical, biological, radiological, and nuclear (CBRN) material

Similar to explosives, there is an existing risk of terrorists carrying CBRN material into airports and airplanes. The release of CBRN substances can easily go unnoticed and quickly spill over to a crucial threat to national security. The agent can show its lethality immediately or over several days or weeks. On its victims and the environment, it can have a severe long-lasting, socioeconomic impact.

The 1995 Sarin attack by the Aum Shinrikyo group on the Tokyo subway showed that attacks with a CBRN agent are not an impossible scenario. The incident resulted in eight casualties and 5510 people reported to hospitals with various complaints. After the Anthrax attacks on the postal office and Senate in Washington, D.C. in the aftermath of 9/11, it took several years and cost over € 1 billion to decontaminate the sites.

Insider threat

The challenge of inhibiting the carrying of hazardous substances into airports and airplanes is closely linked to the insider threat that many providers of public transportation are facing today. With the large number of external service providers working at airport, it is very important to assess potential loopholes for security breaches.

Following the Brussels bombings, the police at Brussels Airport have claimed that at least 50 ISIS supporters are working there as service providers. Officials also revoked the security badges of 70 workers at Roissy/Charles de Gaulle and Orly airports following the November 2015 terrorist attack in Paris.

Cyberattacks

The aviation sector operates with a highly interconnected system of information and communication technology. But, much of the technology currently in use inside of planes was developed at a time when aircraft was not directly linked to the outside world, so most of the systems were not designed to protect the information they carry.

Unauthorised access to data systems can help bypass security checks, seriously compromise the entire airport functioning or even result in loss of control of aircraft. If the availability or integrity of information systems is compromised, it has a profound impact on decision-making processes that are at the heart of airport and aircraft management. Past incidents such as the 'Wanna Cry' attack show that the impact of such disruptions on Critical Infrastructure can be quite significant.

Unmanned Aerial Vehicles (UAVs)/Drones

Another technology that can seriously compromise security checks at airports and directly threaten aviation security is drones. UAVs can circumvent security measures around landside and airside security perimeters, severely compromising aviation security.

When coming close to departing or landing aircrafts, drones represent a lethal security threat. UAVs are already causing widespread disruption at airports today. They halted air traffic at Dubai International Airport three times last year, and similar incidents were reported from London Gatwick airport.

Legislation

Aviation is by far the most regulated transportation mode. The level of harmonisation of the EU aviation security framework is a direct consequence of the 9/11 attacks in the US and has remained very reactive to actual attacks or threats.

Common rules for European Member States were established in 2002 with the adoption of framework Regulation 2320 / 2002[4]. Driven by the need to meet evolving risks in a flexible manner, the initial Regulation was replaced by Regulation 300 / 2008[5], and further supplemented by Regulation 2015 / 1998[6].

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:355:0001:0021:EN:PDF
[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:097:0072:0084:EN:PDF
[6] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1998&from=DE

Regulation 300 / 2008

The Regulation establishes common rules to protect civil aviation against acts of unlawful interference. It sets common basic standards that are much more detailed than in other transportation modes, as they cover:

→ Screening of passengers, cabin baggage and hold baggage;

→ Categories of prohibited articles;

→ Airport security (access control, surveillance, criteria for defining critical parts of security restricted areas and security operations within);

→ Aircraft security checks and searches;

→ Screening of cargo and mail;

→ Screening of airport supplies;

→ Staff recruitment and training;

→ Quality control and oversight measures.

Following Regulation 300 / 2008, Member States must designate a single authority competent for aviation security and set-up a national civil aviation security and quality control programme. Operators are responsible for the definition and implementation of an airport security and air carrier security programme. The European Commission also established the Regulatory Committee for Aviation Security (AVSEC) and the Stakeholder Advisory Group on Aviation Security (SAGAS).

Supplementary regulations and Regulation 2015 / 1998

As a result of the attempted terrorist attack on Northwest Airlines flight from Amsterdam to Detroit in 2009, which involved explosives concealed on a passenger, several supplementary regulations entered into force covering liquids, aerosols and gels; the use of security scanners; the adoption of alternative security measures; domestic and international controls of air cargo ; the specifications of national quality control programmes; and procedures for conducting inspections of the European Commission in the field of aviation security. In 2015, the whole set of previous legislation was updated with Regulation 2015 / 1998 that clarified and strengthened the implementation of common basic standards on aviation security.

The Regulation sets basic rules and standards that are more extensive than in other transportation modes and strengthens measures introduced by Regulation 300 / 2008. However, it still leaves room for derogation, leading to different interpretations across Member States.

Standards

In addition to the aforementioned catalogue of EU legislation, a number of standards applicable to security personnel exist but are often not followed.

Minimum standards for providers of aviation and airport security services

Standard EN 16082: 2011[7] for aviation and airport services specifies quality requirements in organisation, processes, personal and management of a security service provider and/or its independent branches. It sets forth quality criteria for the delivery of civil aviation security services requested by public and private clients or buyers.

The standard is fit for the selection, attribution, awarding and reviewing of the most suitable provider of civil aviation security services.

While the standard has existed for many years, it is hardly used by buyers. It is recommended that this Standard be promoted and adequately highlighted by the European Commission to the European aviation and airport community.

ASSA-i and CoESS Best Value Manuals

A best value manual aiming to help buyers of private security services to select appropriate providers based on objective quality criteria has been developed and published by ASSA-i and CoESS. The CoESS Best Value Manual[8] has been updated in 2015 in cooperation with the European services workers union (UNI Europa) and with financial support of the European Commission, in order to be in line with the new EU Public Procurement Directive. The ASSA-i manual has not been updated, as the CoESS-UNI Europa manual is appropriate for aviation and airport security services. For more information about the manual, please visit **www.securebestvalue.org**.

The ASSA-i Quality Charter and Annex on Training

The Quality Charter has been published in 2008, and has served as a basis for the above-mentioned EN Standard 16082:2011. The Annex on training lists the content of training modules, which PSC staff in airports and aviation should complete in order to reach their operational readiness and capacity beyond basic aviation security training requirements.

Cooperation between Stakeholders

Cooperation on EU-level

The Regulatory Committee for Aviation Security (AVSEC), consisting of experts representing all Member States, was created by Regulation 300 / 2008 and assists the European Commission in its functions and activities.

The Stakeholder Advisory Group on Aviation Security (SAGAS) is the only structural cooperation forum on local, national or European level between public and private security services. In this forum, members assist the Commission in the preparation of legislative proposals and initiatives and can express their views on the work of AVSEC.

Further to the 2015-2016 wave of attacks in Europe, the exchange of intelligence between the EU Member States and between the EU and non-EU intelligence services has been identified as work in progress. There is no way to know if this has actually improved in general with a view to anticipate threats, or if this cooperation is focused on post-attack enquiries, as in the case for Belgium and France, for example.

---

[7] ASSA-I (2011). Projects and Standards. EN Standard. Available at: http://www.assa-i.org/project-and-standards.php?page=en-standard (retrieved: 25.09.2017)

[8] http://www.securebestvalue.org

Stakeholder cooperation in practice

To ensure an effective security chain across stakeholders, it is crucial to ensure a valuable exchange of information and efficient communication across law enforcement, security authorities, airports, carriers, and security service suppliers. But, the presence of a large variety of stakeholders remains a challenge. Airside and landside security are subject to different authorities, with law enforcement and security authorities playing an increasing role in areas of landside airport infrastructure – a situation that can lead to insufficient coordination between all stakeholders.

Stakeholders all have very different and specific interests and the balance between passenger facilitation and security is a delicate one to achieve. However, ensuring the security and safety of airports should be of highest priority, as attacks are highly disruptive and can have a long lasting effect on all airport stakeholders. The improvement of cooperation and communication among aviation security stakeholders should therefore be a priority.

Cooperation with PSCs

Currently, the private security industry is not closely involved in airport security planning by the various responsible public security stakeholders. Also, the legal framework in place in the Member States often does not support the setting up of a two-way open channel of communication for PSCs and relevant law enforcement and/or intelligence authorities.

At the same time, there are also barriers for PSCs to provide information to authorities, as the security industry handles classified information for a number of clients and undertakes assignments in locations where there is a statutory duty of confidentiality.

Gaps and CoESS Experience

Based on evolving risks and existing legislation, standards and their implementation, PSCs in aviation and airports represented by ASSA-i have the following concerns:

Incident-driven legislation

Since the harmonisation of EU aviation security legislation, regulatory developments are incident-driven. European legislation on aviation security currently lacks a suitable response to evolving risks such as insider threats, CBRN, non-metal weapons made out of ceramic and 3D printing, drones and cyberattacks.

Variations in the interpretation of legislation across Member States

CoESS and ASSA-i consider that there is still too much room for interpretation in the common basic standards, leaving considerable gaps. The interpretation of existing aviation security legislation varies from one Member State to another. Without a more global approach and a clarification or simplification of standards, there remains a lack in legal clarity and common interpretation of the legislation, leaving loopholes for criminal networks.

Airports continue to use cost as main criteria in call for tenders

No specific rules exist for public procurement for Critical Infrastructure. As a consequence, contracting authorities often select private security providers on the basis of cost criteria, not on quality of service deliverables. Until now, existing norms, standards and guidelines are only poorly followed.

Liability from acts of terrorism is not harmonised and must be addressed

Another important legislative gap is the inexistence of a harmonised liability regime for the consequences of terrorist attacks. In the event of a terrorist attack, PSCs are not able to face possible third parties' claim, which could relate to amounts exceeding available insurance coverage.

Insufficient coordination and communication between aviation security stakeholders

One of the main challenges to aviation security is the presence of multiple stakeholders. Insufficient coordination and communication among those stakeholders along the security supply chain considerably weakens aviation security measures in place.

In particular, the legal framework in the Member States does not support the setting up of a two-way open channel of communication for PSCs and relevant law enforcement and/or intelligence authorities. This can contribute towards operational bottleneck, when PSCs provide information to the police and little or no information is returned, because PSCs do not have an authorisation to receive sensitive information from the police or intelligence services. As PSCs often represent first in line prevention services and response in case of an incident, this is a serious shortcoming in legislation.

Future Developments

As indicated in our risk assessment, the threat environment for aviation security is evolving. New technologies are increasingly posing a challenge to airport operations, while returning ISIS fighters and 'home-grown' radical Islamists can be expected to plan further attacks on European soil. These developments make a pro-active legislative approach that anticipates these threats necessary.

As technology becomes more sophisticated, CoESS also stresses that there needs to be a strong focus on the human factor.

HME's and IEDs

The recent incidents in Brussels (2016) and Barcelona (2017) show that terrorist networks have sophisticated bomb-making capabilities and can be expected to use HMEs for future attacks. US officials warn that explosives could, for example, be hidden in computers and can evade detection by scanners.

Therefore there is a need to adequately address the risk of attacks including IEDs being concealed in cabin or hold luggage.

Insider Threat

As explained in our risk assessment, the insider threat considerably weakens existing security measures. There are no technological means to avoid and detect risks originating from insider threats. Best practices, for example of the Federal Bureau of Investigation (FBI), refer to management practices and recommend having a solid 'Insider Threat Team' in place. While technology can help, only people can effectively develop and apply such kind of safety and security at work policies.

New technologies: cyberattacks and drones

The challenge that possible cyberattacks and drones pose to aviation security is very likely to increase. The frequency of large-scale cyberattacks on business and Critical Infrastructure increased tremendously in 2017, while incidents with drones intruding airport perimeters have already occurred at numerous airports. As a reaction, France has already introduced stricter security measures for the operation of drones, including a weight threshold of 800g, a capacity limitation for a maximum altitude of 150m, and an obligation for audible warning systems.

CoESS is therefore in favour of a new drones' regulation, as proposed by the European Aviation Safety Agency (EASA) in NPA 2017-05[9]. However, we strongly recommend that more attention is given to the security of drones, and that regulation is introduced following targeted security risk assessments.

Conclusion and Recommendations

We strongly recommend implementing additional security measures and a legislative framework that pro-actively responds to evolving threat environments and does not leave room for different interpretations. Furthermore, it is crucial to strengthen the security supply chain by means of better exchange of information across all involved public and private stakeholders, mandatory compliance with procurement standards and a framework that guarantees a harmonised liability regime for the consequences of terrorist attacks.

Additional screening measures to anticipate emerging threats

There is a need to adequately address the risk of attacks using IEDs that can be concealed in cabin or hold luggage. The specific issue of IEDs is handled in a separate document with restricted circulation, which has been sent to the appropriate services within DG MOVE and DG HOME.

Passenger and cabin baggage
We advise implementing additional security measures concerning the use of Explosive Trace Detection (ETD) equipment. Such measures will systemise current operational procedures at European Airports to effectively react to positive ETD alarms during passenger and cabin baggage screening processes.

Furthermore, hand search only for security control methods of cabin baggage should no longer be allowed in order to efficiently respond to the modus operandi of terrorist organisations.

[9] https://www.easa.europa.eu/system/files/dfu/NPA%202017-05%20%28A%29_0.pdf

Hold baggage

Adequate procedures for the security control of hold baggage are crucial. Especially in cases where hand search is the primary and only method, the additional application of ETD methods should be mandatory.

Vehicles

We further advise adding, on a mandatory random/unpredictable basis, elements of security controls for vehicles accessing critical parts of security restricted areas by means of ETD equipment – especially with regard to vehicle interiors. Currently, these can be used as supplementary methods only.

Airport suppliers

In light of current threats, security controls of airport supplies should be tightened to reach higher detection levels. Current regulatory standards are far too liberal towards security control requirements of unknown airport suppliers. Vetting of staff needs to cover not only staff security but also staff from airport suppliers and sub-contractors, as well as handling companies. Cleaning, catering, mail offices, maintenance, hotels, parking, retailers – they can all be targets for future insider threats.

Address variations in interpretation of EU legislation

Certain aviation security measures should be clarified, harmonised or simplified in order to improve legal clarity, standardise the common interpretation of the legislation and further ensure the best implementation of the common basic standards on aviation security.

Pro-active EU legislation

Regulatory developments of EU aviation security legislation have always been incident-driven. Legislative initiatives should become more pro-active, pre-empting and anticipating scenarios including new types of attacks using HMEs and IEDs, insider threats, CBRN, drones and cyberattacks. As a first step, the definition of airport landside operations should be adequately extended to take into consideration new types of threats, corresponding to today's reality.

Additional security measures for airport's landside infrastructure

AVSEC regulatory standards need to take additional measures into consideration that aim to effectively protect soft targets and other vulnerable elements of airport's landside infrastructure, depending on a local risk assessment. Additional measures should be taken into consideration for the protection against and response to CBRN or cyber threats.

CBRN preparedness

To anticipate current threat developments, all aviation security providers, especially those first in line, should be familiar with basics of CBRN protection and contingency. We therefore strongly recommend the introduction of additional mandatory training measures and standards.

Mandatory criteria and standards for the procurement of private security providers

Enhanced security in airports and aviation starts with the selection of private security providers that comply with the common quality criteria. Airports, as with any Critical Infrastructure, should be subject to different criteria in public procurement of security services. At least 50% of the assessment should be quality-based driven criteria referring in particular to aspects such as security training, quality control and compliance assurance, implementation of technological developments and contract management.

ASSA-i and CoESS assist buyers of private security providers in identifying quality criteria, mainly by:

→ providing a best value manual entitled "Buying Quality Private Security Services"[10]. The guide can be downloaded here: www.securebestvalue.org.

→ assisting in the development of an EU norm, EN 16082:2011, outlining minimum standards for providers of aviation and airport security services.

We strongly recommend that compliance with EN 16082:2011[11] is made mandatory for security service suppliers in airports and aviation.

Additionally, and aiming to improve the aforementioned initiatives, establishing a European PSC Certification Programme for all private security providers offering their services within EU aviation security could be required. Such a certification model would be important to guarantee that all stakeholder organisations involved in airport security throughout the EU are fully compliant with mandatory practices and procedures.

Harmonised liability regime for the consequences of terrorist attacks

CoESS and ASSA-i call for a fair and acceptable distribution of responsibilities and risks between the authorities and other parties responsible for security, on the one hand, and PSCs to which security services have been outsourced, on the other hand. Only a clear EU initiative, possibly leading to a common legal framework, or joint strategy by the Member States, will be able to efficiently address the issue for all different sectors concerned.

Exchange of information among public and private security stakeholders

Resources dedicated to intelligence need to be reinforced in such a way that attacks can be anticipated and avoided. PSCs can play an important role in this effort as they are usually the first line of response for the most of threats and current modus operandi of terrorists, and intelligence services will not always detect the forthcoming attack.

The private security industry should therefore be more closely involved in airport security planning to form an effective and smooth security chain. A clear framework needs to be established for the exchange of relevant information between PSCs and law enforcement/intelligence agencies – bearing in mind data protection and privacy regulatory frameworks.

---

[10] http://www.securebestvalue.org
[11] http://www.assa-i.org/project-and-standards.php?page=en-standard

To support such a framework, PSCs should be able to establish an effective sensitive data sharing system between law enforcement and intelligence agencies. Therefore, the European PSCs Certification initiative should take place, aiming to specify requirements and conditions under which PSCs shall be able to operate within aviation security and other Critical Infrastructure environment.

Each PSC working in aviation security services should appoint a Civil Aviation Security Intelligence Director, acting as a sole point of contact for law enforcement/intelligence agencies designated Officers, assuring the compartmentalisation of relevant information. The establishment of internal corporate intelligence units could further facilitate communication between PSCs, their clients, and law enforcement units.

Security culture

Smooth cooperation and communication between all stakeholders is a key factor for a successful security policy and operation. If security is to be taken seriously, it can only be within a dynamic process (Plan Do Check Act mode), where security – as well as safety - is considered as a chain, within which each stakeholder knows its own mission, duties, role and responsibilities and understands, uses and supports smooth and effective processes. This will promote communication that follows a clear and efficient path so that security can be improved in a constant way.

Developing a security culture in airports is an area where people matter more than technology. Creating a security culture, not only within the staff of all stakeholder organisations, but also with passengers, is a winning strategy in anticipating both security and safety issues. For all staff, stakeholders and passengers, the principle of "if you see something, say something" needs to be repeated on a regular basis to keep everyone alert to possible dangers and informed on how and to whom issues should be reported.

Smart Security Concepts

Developing smart security concepts is also an area where cooperation from all stakeholders gives better results than working in isolation. There are examples where, for example, guards were consulted prior to developing new, so-called "smart security" concepts, giving excellent results and high motivation levels.

Maritime Security

Executive Summary

An open and protected sea is a crucial pillar for free trade and an important source of economic prosperity and mobility in Europe. Hundreds of millions of citizens pass through European ports and maritime infrastructure each year and almost 90% of Europe's external freight trade is sea-borne.

Maritime infrastructure is vulnerable to a complex threat environment, ranging from smuggling to terrorist attacks. A comprehensive legislative framework exists to protect the citizens and our economies from the consequences of unlawful intentional acts against shipping and port operations. Still, gaps remain in its implementation. Standards for training and procurement of security personnel are non-existent, responsibilities of security guards that are often first in line are restricted and security measures in different modes of transport vary widely and do not respond to new technologies in the hand of criminal and terrorist networks.

CoESS recommends aligning maritime security measures with aviation standards and to respond to new means of unlawful intentional acts, including cyberattacks or drones, in a pro-active and preventive approach. To create a stronger security culture among maritime stakeholders and staff, and to anticipate and avoid serious incidents, stronger standards for trainings and procurement need to be introduced. Additionally, sharing of information and best practices among public and private security stakeholders is key to enhance the security of maritime infrastructures and transportation modes.

Introduction

The functioning and safety of maritime infrastructures is key for trade, logistics, mobility and tourism in Europe. Hundreds of millions of citizens pass through European ports and maritime infrastructure each year and almost 90% of Europe's external freight trade is sea-borne.

But, maritime infrastructure also faces a complex threat environment that will be assessed in this chapter before discussing gaps in existing standards, legislation and their implementation. We will make proposals on how to improve maritime security measures, legislation and standards based on our experience and identified gaps.

Our comments and recommendations are limited to shipping and port operations **within the European Member States** and do not include protection of ships in high-risk areas outside Europe.

Risk Assessment

Maritime infrastructures are vulnerable. The evolving terrorist threat on means of transportation; maritime piracy; illegal immigration; the proliferation of arms and hazardous substances; unlawful intentional acts by means of cyberattacks and drones – these increasingly complex risks and challenges to maritime security make an update of European policies and their better implementation necessary.

When talking about risks, we distinguish between:

Passenger ships (such as ferries or cruise ships)

With hundreds of millions of Euros invested in each vessel and the congregation of a large number of passengers, ferries and cruise ships represent a vulnerable target for terrorist groups – similar to airplanes and mass land transportation networks. Means of attacks can include firearms, HMEs, IEDs or even CBRN.

Until today, there has not been a terrorist attacks on board passenger ships in Europe. But, the bomb attack on the Philippine Superferry14 in 2004 shows that such an incident would immediately affect a large number of people, attract a lot of media attention and would have severe consequences for tourism, mobility, and trade.

Cruise ships therefore have very strict security guidelines based on the International Maritime Organisation's (IMO) International Ship and Port Facility Security (ISPS) Code. Like in aviation, even at Risk Level 1, 100% of the passengers and their hand-luggage are to be screened by metal detectors. Passengers remain exposed though when they are onshore, especially when they are in large groups in the port terminals (pre-boarding) and during organised visits.

While ferries operate in a similar threat environment, they do not systematically screen boarding passengers, their hand-luggage and vehicles – leaving people on board vulnerable to attacks with firearms and explosives.

Cargo ships

Maritime trade is the backbone of Europe's economy, but cargo ships and their freight are difficult to monitor and scan entirely – a deficiency that has long been exploited by organised criminals. Cargo remains a very vulnerable target for criminal acts such as illegal immigration, human and drugs trafficking, proliferation of weapons, piracy and terrorist attacks.

An incident with a cargo ship, especially when loaded with hazardous substances, can have long-lasting consequences, harming people and the environment in the port itself and in greater metropolitan areas, crippling the port activities and the country's economy.

Recent tragic events on the Norman Atlantic in the Adriatic Sea show that there is a need to ensure the security of passengers and cargo, as security risks may have serious safety implications.

Offshore structures

Fixed offshore structures, such as wind turbine parks with sub-stations or drilling platforms in the European Economic Zone, are not subject to any specific security regulations. However these structures can play a critical role in the energy supply of the Member States and are increasingly dependent on programmable control systems. An incident, including cyberattacks, can have severe economic and environmental consequences.

A cyberattack on an oilrig, for instance, can result in more than just lost revenue – it can be catastrophic for the environment and have far-reaching ramifications. Offshore platforms in Saudi Arabia and Iran have been targets of cyberattacks in the past, leading to an interruption in oil supply that can for some countries be a matter of national security. Examples like the 'Wanna Cry' attack in May 2017 show that European offshore structures, for example in the North Sea, could easily be the target of future incidents.

Seaports & Terminals

Many European terminals and ports function as trade hubs and are Critical Infrastructure that faces similar threats to airports. They are a key facilitator in European trade, logistics, and transportation. But today, they also continue to be in many cases vulnerable to security incidents, especially intrusion in IT systems and terrorist attacks, which can disrupt traffic and trade flows causing significant economic impact.

Minor incidents can quickly escalate to a major crisis, having an impact on a large amount of passengers and personnel, the environment, trade and national security.

Examples of incidents can include evacuation of illegal immigrants, loss of electrical power, water and communication systems, fire and explosions, major structural failure, spills of flammable or CBRN material, and criminal activity including terrorist activities on personnel and large passenger groups.

Important threat developments are drones that can circumvent security measures around the port security perimeter, severely compromising security, and insider threats. As an example, in September 2017 a report of Antwerp Police in Belgium warned that drug cartels have infiltrated businesses, customs, and the police itself.

Inland ports and terminals, with cargo to/from seaports

The risks to the economy and trade of inland ports are similar to seaports, however an important gap in security requirements exists between the two.

Legislation

Following legislations and regulations are relevant to security services	Pax Ships	Cargo Ships	Off shore	Sea Ports	Inland Ports
ISPS CODE	X	X		X	(1)
Maritime Security Regulation 725 / 2004	X	X		X	(1)
Port Security Directive 2005 / 65				X	
AEO Regulations 648 / 2005				(2)	

Notes: (1): if / when receiving seagoing ships
(2): for certified terminals

The overall objective of the EU's maritime security policy is to protect European citizens and economies from the consequences of unlawful intentional acts against shipping and port operations.

The legislative framework is based on the ISPS Code that provides minimum international requirements for the security of ships and ports. The EU has complemented the ISPS Code with Maritime Security Regulation 725 / 2004[12], Port Security Directive 2005 / 65[13], and Authorised Economic Operator (AEO) Regulation 648 / 2005[14].

ISPS Code

The ISPS Code is a mandatory instrument for all countries Party to the IMO's International Convention for the Safety of Life on Sea (SOLAS)[15]. It guarantees that ships and port facilities are implementing minimum international standards of maritime security and contains mandatory security-related requirements for governments, port authorities and shipping companies at national, regional and international levels. It includes:

→ a framework to assess and detect potential security threats to ships or port facilities, and to implement preventive, adequate, and proportionate security measures against such threats;

→ a definition of roles and responsibilities of all parties concerned with safeguarding maritime security in ports and on board ships;

→ mechanisms for early and efficient exchange of maritime security-related information;

→ methodologies for ship and port security assessments to facilitate the development of ship, company and port facility security plans and procedures, which must be utilised to respond to ships' or ports' varying security levels;

→ a definition of security levels and respective preventive measures.

The ISPS Code also includes a series of non-mandatory guidelines in its Section B.

---

[12] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:129:0006:0091:en:PDF
[13] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:310:0028:0039:EN:PDF
[14] https://ec.europa.eu/taxation_customs/general-information-customs/customs-security/authorised-economic-operator-aeo/authorised-economic-operator-aeo_de
[15] http://www.imo.org/en/About/conventions/listofconventions/pages/international-convention-for-the-safety-of-life-at-sea-(solas),-1974.aspx

Maritime Security Regulation 725 / 2004

The main objective of the Regulation[16] is to ensure harmonised interpretation of the ISPS Code among EU Member States. Furthermore, it makes a number of non-mandatory recommendations mentioned in the ISPS Code Section B mandatory for governments, port authorities and shipping companies.

The Regulation is limited in scope to security measures on board vessels and the immediate ship/port interface. Member States can determine for which kind of domestic ports and ships, except for Class A passenger ships, the Regulation applies.

Applicable Maritime Security Levels are set by national authorities and are defined as:

→ **Security Level 1** means minimum appropriate protective security measures to be maintained at all times.

→ **Security Level 2** means appropriate additional protective security measures maintained for a period of time as a result of a heightened risk of a security incident.

→ **Security Level 3** means further specific protective security measures maintained for a limited period of time when a security incident is probable or imminent.

LEVEL 1	LEVEL 2	LEVEL 3
Ensuring the performance of all ship security duties	Assigning additional personnel to patrol deck areas during silent hours to deter unauthorised access	Limiting access to a single, controlled, access point
Access control to ships	Limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them	Granting access only to those responding to the security incident or threat thereof
Embarkation control of passengers	Deterring waterside access to the ship, including, for example, in liaison with the port facility, provision of boat patrols	Directions of persons on board
Monitoring of restricted areas	Establishing a restricted area on the shore-side of the ship, in close cooperation with the port facility	Suspension of embarkation or disembarkation

---

[16] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:129:0006:0091:en:PDF

Monitoring of deck areas and areas surrounding the ships	Increasing the frequency and detail of searches of persons, personal effects, and vehicles being embarked or loaded onto the ship	Suspension of cargo handling operations and deliveries
Supervision of cargo handling and ship's stores	Escorting visitors on the ship	Evacuation of the ship
Ensuring that security communication is readily available	Providing additional specific security briefings to all ship personnel on any identified threats, re-emphasising the procedures for reporting suspicious persons, objects, or activities and stressing the need for increased vigilance	Movement of the ship
Ensure liaison with the Port Facility to ensure designated secure area for inspection and searching	Carrying out a full or partial search of the ship	Preparing for a full or partial search of the ship

Mandatory security measures according to Maritime Security Regulation 725 / 2004.

Port Security Directive 2005 / 65

The Directive[17] introduces a security regime for ports and its personnel, passengers, infrastructure, and equipment, improving security in areas of ports not covered by Maritime Security Regulation 725 / 2004[18]. It applies to the entire perimeter of port activity and includes guidelines, mechanisms and requirements for port security assessments and port security plans.

Member States have to determine, on the basis of their security assessments, which ports are concerned and which alternative measures provide an adequate level of protection.

Authorised Economic Operator (AEO) Regulation 648 / 2005

In the area of international trade in goods, customs authorities in the EU apply a risk-based approach to security threats based on AEO Regulation 648 / 2005[19]. Within the AEO concept, traders who voluntarily meet a wide range of criteria work in close cooperation with customs authorities to assure supply chain security.

Regulation 648 / 2005 creates a legal basis for harmonised and recognised supply chain security standards and custom controls across the EU. It defines criteria for authorised economic operators, and a framework for custom controls.

[17] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:310:0028:0039:EN:PDF
[18] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:129:0006:0091:en:PDF
[19] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:129:0006:0091:en:PDF

Standards

As mentioned, Maritime Security Regulation 725 / 2004 makes mandatory certain articles of Section B from the ISPS code. These specifically concern the Port Facility Security Assessments (PFSA) and Security Trainings.

With regards to training, we notice that standards often vary among Member States or are even missing. A few examples:

Port Facility Security Officers (PFSO)

The ISPS code lists the topics that a person needs to be familiar with before taking on a role as PFSO. IMO developed a recommended Model Course (3.21) for such training. However when it comes to implementation, no standards exist to test that PFSO's have the required knowledge to perform their tasks. Concrete approval requirements for training material and trainers exist only in a limited number of Member States, resulting in important quality differences between training institutes.

Personnel with security tasks (Guards)

Similar to PFSO's, security personnel must demonstrate knowledge of the topics listed in the ISPS Code (Art. B18). However, some Member States do not require extra training for security guards working in seaports. Concrete standardised requirements for approval for training material and trainers only exist in a limited number of Member States.

CoESS has developed a training manual that can be used on a voluntary basis by the private security industry to train guards working in seaports. A wider promotion, similar to the European Handbook of Maritime Security Exercises and Drills (Exercitium) developed by the Port of Antwerp with support from EU, should ensure to train personnel with security tasks to the right level.

Guard force management and standards

CoESS has been deeply involved in the development of a European Norm for Maritime and Port Security Services. The EN Norm 16747:2014 was elaborated within the European Committee for Standardisation (CEN) by maritime security experts to harmonise port security services across CEN countries. It establishes minimum quality criteria for recruiting, vetting and training people, and for contract and service level management.

Certification based on EN 16747:2014 is voluntary, but we strongly recommend that all public and private seaports verify compliance with the norm when training in-house security or contracting private security services.

Best-value procurement

Public stakeholders often award contracts to private security providers mainly on the basis of cost criteria, not on quality. CoESS therefore assist buyers of private security providers in identifying quality criteria with a best value manual entitled "Buying Quality Private Security Services"[20]. The guide has been updated in 2015 in cooperation with UNI Europa and with financial support of the European Commission, in order to be in line with the new EU Public Procurement Directive. For more information about the manual, please refer to **www.securebestvalue.org**

Cooperation between Stakeholders

Cooperation on EU-level

The Regulatory Committee for Maritime Security (MARSEC), consisting of experts representing all Member States, was established by Maritime Security Regulation 725/2004 [21] to assist the European Commission in its functions and activities. Best practices and indications on national instructions are shared in this forum, and a mechanism to secure mutual sharing of sensitive information has been recently created.

The Stakeholder Advisory Group on Maritime Security (SAGMAS) is the only structural cooperation forum on local, national or European level between public and private security services. In this forum, members can express their views on the work of MARSEC.

Stakeholder cooperation in practice

On practical level, communication along the security supply chain is crucial and can be improved. An exchange of information and efficient communication must be assured across law enforcement, security authorities, ports, carriers, and security service suppliers to set in place a functioning security culture – also with regard to insider threats. The presence of a large variety of stakeholders, similar to the aviation sector, remains a challenge.

Gaps and CoESS Experience

The CoESS Maritime Security Committee meets regularly with maritime security experts for an exchange of views. The latter frequently raise the following points of concern, based on their contacts with the port authorities and private port operators:

Gaps in security measures in different modes of maritime transport

Following the risk assessment, legislative frameworks and security measures introduced at ports are not pre-emptively responding to an evolving threat environment. Particularly, variations in security measures at different modes of maritime transportation and trade represent important gaps in the maritime security framework in practice.

Ferries or Pax-Ro ferry terminals
The difference in security between similar-size terminals used by passengers travelling by air and by sea for instance is considered as the main gap. Ferries and Pax-Ro terminals check the boarding passes to ensure the fare was paid. There are no full-scale security checks of vehicles, luggage (X-Ray) and persons (walk-through metal detectors), allowing criminals to embark easily with firearms or explosives that can be used against defenceless passengers trapped on-board a ship.

Cargo ships
The security of cargo ships requires more focused attention. The ISPS code falls short of mandating specific security standards. It is important that cargo ships have strict security guidelines, are well protected, and have crews that are well prepared to confront security concerns until first-responders can address the situation.

[20] http://www.securebestvalue.org
[21] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:129:0006:0091:en:PDF

Inland ports

Furthermore, there are clear gaps in the security of inland ports when compared with seaports – for instance in supply chain security. The risks to the economy and trade are similar and concerns related to the theft of cargo and the facilitation of smuggling are big.

Variation in maritime security expertise of PFSO across Member States

As previously mentioned, no standards exist among Member States to assess whether a PFSO has the required knowledge to perform their tasks. The know-how between PFSO's therefore often varies radically. Our experts and we frequently encounter PFSO's that aren't familiar with the risk-based approach and ISPS obligations, or who were trained nearly 15 years ago and are no longer familiar with the current security thinking and technology. This is a crucial shortcoming in the current maritime security setting, particularly in a constantly evolving risk environment.

Variation and restriction of tasks performed by security guards

To comply with Port Security Plans, ports and terminals employ security guards. But in reality, the tasks performed are not always security related. For example, guards used at the gates for the check of the documents don't have time or are not instructed to check the inside of the truck or under and on top of the trailer.

Furthermore, PSCs are often prohibited by Member States' laws to intervene in the public area apart from reporting suspicious activities. For example, in cases where illegal migrants try to get on board of vessels as stowaways, PSCs often can only act when they notice effective trespassing of the terminals' perimeter. Following such a reactive approach is much less effective and more dangerous for migrants and security staff than a pro-active approach that prevents trespassing in the first place.

Security procurement with price-only focus

Another problem that security providers at ports face, similar to airports, is that suppliers are often selected by port terminals at below-cost prices. CoESS therefore promotes the Best Value approach (**www.securebestvalue.org**) to select a security provider.

Liability from acts of terrorism

Similar to other transportation modes, a harmonised liability regime for the consequences of terrorist attacks does not exist. In the event of a terrorist attack, PSCs are not able to face possible third parties' claim, which could relate to amounts exceeding available insurance coverage.

Future Developments

These gaps become urgent to address in an evolving threat environment. Emerging security risks are diverse depending on the mode of maritime transportation, the type of ports, and technologies in the hands of criminal and terrorist networks.

Terrorist networks, including insider threats

With a congregation of a large number of passengers and a variety of external service providers and business involved, ferries, cruise ships and terminals represent a vulnerable 'soft target' for terrorist groups – similar to airports and airplanes. Transportation systems have long been a target for terrorist attacks. An incident immediately affects a big amount of people, attracts a lot of media attention and can have severe consequences for tourism, mobility, and trade. It is important that the maritime infrastructure is as much prepared for risks related to HME, insider threats and attacks with any kind of arms as the aviation transportation sector.

Drones

The greater use and availability of drones is also a very important development in the maritime threat environment and requires greater attention. When in the hand of criminals or terrorist groups, drones can circumvent security measures around the ship and port security perimeter, severely compromising their security independently from Security Levels. They can transport prohibited items (for instance fire arms and drugs) between ships and shore, and could be used to organise an attack with explosives. Port and Ship Security Plans do not as of yet cover these risks, however PFSO and security providers need to be put in the position to properly deal with them. Airborne attacks, either with drones carrying explosives or with improvised mortars, make passenger ships highly and particularly vulnerable[22].

Cyberattacks

Unauthorised access to data systems by criminals can have implications for the prohibition of smuggling and trafficking of persons, arms, and drugs. Cyberattacks can further have severe consequences for the proper functioning of ships, ports, and offshore structures. Past incidents on other Critical Infrastructures such as the 'Wanna Cry' attack show that such scenarios can lead to serious economic and environmental consequences.

Conclusion and Recommendations

We do not recommend major changes in existing laws and regulations, but we strongly endorse an alignment of security standards at seaports and airports which both face very similar threats. European legislation on maritime security should become more pro-active, pre-empting threat scenarios including drones and cyberattacks. Further, the application of existing laws and regulations should be better controlled, guaranteeing standardised training and knowledge of port security personnel and PFSO's across Member States. PSCs can be important partners in these efforts.

[22] Attacks took already place in Europe, but not yet against maritime targets

Aligning maritime and aviation security standards

Our overall recommendation is, for passenger security, to align seaports security standards with airports standards. The same applies for the security of inland ports that should be further in line with standards at seaports to inhibit the theft of cargo and smuggling.

The protection of cruise and ferry passenger terminals should be at a level that is similar to airports as both face similar security challenges and vulnerabilities. For example, an international screening standard should be created and used similar to aviation security. Such a measure would ensure that passengers in seaport terminals are screened in a similar manner, preventing attacks on vessels. Also, this will increase acceptance and throughput efficiency in order to minimise delays.

Applying the ISPS more stringently would also mean enforcing effective random/unpredictable searches for vehicles and passengers embarking on ferries – even at Security Level 1.

Amendments of Port Security Directive 2005/65

Concrete regulatory amendments could be incorporated in the Port Security Directive 2005 / 65[23]. Based on the current and future development of threat environments, we strongly recommend protecting communication systems and cargo data against cyber criminality. The airspace above ships and ports should be safeguarded against unwanted drone incursions, and fixed offshore structures should be protected against any kind of conventional and non-conventional attacks to secure staff, energy production and environmental protection.

Training, certification processes and tasks

We do not recommend major changes in other existing laws and regulations, but their stricter application and control across all Member States, especially with regards to the training and certification processes of PFSO's and port security personnel. A good practice for the approval of PFSO training exists, for instance, in the United Kingdom, while recommendable Port Security Guard trainings are in place in Belgium.

When renewing ISPS certifications for port facilities, authorities should verify that Continuous Development Plans are in place to ensure that PFSO and personnel with security duties maintain their skills and security knowledge.

Standards for the procurement of private security providers

Security supply chains are only as strong as their weakest link. Enhanced maritime security therefore starts with the selection of security providers that comply with high quality criteria – similar to our recommendation for airports.

CoESS therefore promotes the Best Value approach (**www.securebestvalue.org**) to select a security provider.

---

[23] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:310:0028:0039:EN:PDF

Public-private cooperation and information sharing

Private security personnel are often first in line in case of an incident. We therefore recommend that the private security industry is more involved in seaport security planning by the various public security players, at least on national level. More resources should be dedicated to information sharing to form a more effective security chain. Knowledge and expertise, lessons learned and best practices should be further exchanged within MARSEC and SAGMAS, improving knowledge sharing among both public and private security providers.

A two-way open channel of communication for private security companies and relevant law enforcement and intelligence authorities ensures that (private) security guards know what to look for when assessing 'suspect' or 'unusual' behaviour. In the planning of attacks, it is a well-known fact that criminals will conduct reconnaissance missions, take notes and pictures, or practice a dry run. Any observation of unusual behaviour could be reported to the adequate authorities in a swift manner, enhancing security at all kinds of maritime transportation modes. There are currently no up-to date statistics to be shared, but an academic study of the port security level would surely be beneficial to authorities, port operators and security companies.

Land Security

Executive Summary

Land transportation is an integral part of European trade and mobility. Millions of passengers use means of public transportation each day; high-speed train networks operate across borders and connect major cities; and land cargo is a backbone of European trade and logistics. But, unlike the aviation and maritime sectors, and except for dangerous goods movement, there is no EU legislation addressing land transport security.

Following the frequency of recent terrorist attacks on passenger transportation, there is scope and justification for a more active European approach to the broad and complex area of land transport security and, in particular to the security of passenger transport. The attacks in the past few years have pointed to the need to better secure train stations and transport hubs in general. Activities of the European Commission, such as the Staff Working Document on Transport Security[24] and the Commission's conference on transport security, are important initiatives that provide the basis for a very fruitful exchange of views and best practices. However, security measures at the Member State level are mostly taken in a post-attack climate, primarily in cities and countries that have been attacked. In countries that have not yet been targeted by terrorist attacks, there is a need to respond to risks in a more preventive way, also in 'quieter' times.

Finally, as we will also explain, coordination among stakeholders along the security supply chain is insufficient, and most of the time clients still select private security providers mainly on the basis of cost criteria, not on quality. CoESS has done much work in order to assist buyers of private security providers in identifying quality criteria, for example by publishing a best value manual[25] in conjunction with UNI Europa, and with financial support of the European Commission.

Introduction

Modes of land transport are crucial for urban, national, and cross-border mobility, as well as trade and logistics. Hundreds of millions passengers use public transportation each day, and European trade heavily relies on land cargo that connects with maritime and aviation hubs.

Particularly passenger transportation is highly vulnerable to terrorist attacks. But also cargo is challenged by risks related to theft and trafficking, and since recently also to new modus operandi of terrorist networks. In this chapter, we will assess the risk environment of land transportation and discuss existing legislative measures and standards, before providing recommendations to respond to the evolving threat environment based on identified gaps.

In this chapter, we will focus on:

➔ Passenger transport by rail (metro and trains), as well as train/metro stations security;

➔ Cargo transport by road and rail.

---

[24] https://ec.europa.eu/transport/sites/transport/files/themes/security/doc/2012-05-31-swd-transport-security.pdf
[25] http://www.securebestvalue.org/

Risk Assessment

Means of public mass transportation such as metros, (sub-)rail networks, high-speed trains and transportation hubs are highly vulnerable soft targets for terrorist attacks. They remain very difficult to secure, and have also in the past years been targets.

Another important part of land transportation security is cargo transport and supply chains. Both play a substantial role in European trade and are exposed to theft, illegal trafficking, and contamination. Further, terrorist groups have increasingly discovered heavy vehicles as an easily accessible and effective weapon against civilians.

For our risk assessment, we distinguish between these two domains of land transportation security.

Passenger transport

According to the European Association for Public Transport (UITP), the public transport sector contributes up to € 150 billion per year to European economies. Every year, metros, trams, light rails, suburban rails, and long-distance trains account for 26 billion passenger journeys in Europe. Urban and suburban public transport carries approximately 185 million passengers on an average working day across the EU, providing the backbone of urban mobility in many EU cities[26].

Such congregation of a large number of passengers qualify public transportation as a vulnerable soft target that is very difficult to secure. Urban mass passenger transportation as well as long-distance trains and related transportation hubs are easily accessible, and it is not difficult for terrorists to conduct attacks with weapons or explosives that will result in a high number of casualties.

Attacks with homemade explosives on urban mass passenger transportation and stations have been proven as highly effective for terrorist networks, as the bombings on the Maelbeek Station in Brussels (2016), multiple metros in London (2005) and sub-urban trains in Madrid (2004) sadly show.

Attacks on train stations and high-speed networks show similar characteristics: In 2012, the German police found a bag with a homemade pipe-bomb at the Bonn train station; and in August 2015, a shooting and stabbing incident took place on-board of a high-speed Thalys train between Amsterdam and Paris.

The 1995 Sarin attack by the Aum Shinrikyo group on the Tokyo subway showed that attacks with a CBRN agent are not an impossible scenario.

ISIS has therefore called upon sympathizers to conduct attacks on public transportation, which makes further attempts in the EU, both by lone actors and groups, very likely to take place in the near future.

Cargo transport and supply chain

Attacks with vehicles as a weapon (VaaW)
The concern is that as soon as an attack has taken place, security measures are adopted as a response and terrorists very quickly change their modus operandi and targets. This trend has been demonstrated by a number of attacks with VaaW across Europe on public, crowded places within only the past year:

[26] UITP (2014). Key Statistics. Available at: http://www.uitp.org/key-statistics (20/09/2017)

→ **July 2016 (France):** On French Independence Day, a 19 tonne cargo truck is deliberately driven into crowds of people celebrating on the Promenade des Anglais in Nice.

→ **December 2016 (Germany):** an ISIS-sympathiser hijacks a semi-trailer truck on a remote parking lot, killing the driver and running over crowds on the Berlin Christmas Market.

→ **April 2017 (Sweden):** a hijacked truck is deliberately driven in a pedestrian shopping district in Stockholm.

→ **June 2017 (United Kingdom):** a van leaves the road on London Bridge and strikes pedestrians, followed by an attack on the London Borough Market.

→ **August 2017 (Spain):** a member of a larger ISIS terrorist group drives a van into pedestrians on La Rambla street in Barcelona.

As a reaction, security measures on local level have been stepped up to better secure public events and pedestrian streets.

Risks along the supply chain
Goods transport plays a fundamental role in delivering goods across countries and regions in Europe. If the supply chain is affected by a security incident, the impact and related costs can be quite significant, in addition to the loss of the merchandise itself and its economic consequences. Indirect costs include the interruption of the delivery chain, the increase in customer care, reparation of the loss, increase in insurance premium, liability and possible loss of customers.

The main threat and concerns of transport companies and owners of goods include:

→ theft;

→ cargo contamination (weapons, drugs);

→ illegal trafficking of people (refugees, human trafficking).

The type of merchandise that is targeted varies: alcoholic beverages, perfumes/cosmetics, pharmaceuticals, textile, tobacco products, foodstuffs, tyres and vehicle spare parts, electronics, metals, etc.

Modus operandi also vary, and include: theft with violence, "surfers' method" (thieves boarding the truck whilst on the move, via a vehicle following the truck), fake policemen, fake accidents, Trojan horse, fake calls, driver swaps, vehicle marking, fake companies, gas or even explosives.

Technologies may be used to support the illegal acts, including frequency disrupters or hacking, for example.

Legislation

European legislation

There is currently no EU legislation addressing land transport security, with the exception of the dangerous goods movement. Following the risk assessment and high number of attacks on metro's, (high-speed) trains, and urban transportation hubs, this presents a gap in the legislative security framework.

An important step towards a European framework on land transport security has been made with the publication of the European Commission's Staff Working Document on Transport Security[27]. It provides an overview of potential areas for the development of EU land transport security policies. In particular, the document highlighted the need to focus on a number of areas, including multimodal transport hubs, high-speed rail network, training of staff, handling and the exchange of classified information, the security of the supply chain, and cyber-crime[28].

More action has been taken on national level following the frequency of recent attacks on land transportation. Current actions mostly focus on international passenger trains and stations, and are very incident-driven.

Example for national security measures and legislation

In the past three years, France has been subject to a high number of terrorist attacks on soft targets including land transportation modes.

As a result of the Vigipirate Plan, a total of 2,800 armed and uniformed agents of the 'Surveillance Générale' are deployed in railway stations and trains across the country. The state-owned public transport operator in Ile-de-France, RATP, further planned to deploy more than 1,000 armed agents which are part of the 'Groupe de Protection et de Sécurisation des Réseaux'. These agents are also allowed to check passenger bags.

Approximately 40,000 fixed cameras are installed in the RATP stations and mobile cameras are also used. As for the SNCF, it deploys over 30,000 cameras in stations and on trains. Intelligent cameras are currently undergoing tests.

After the Thalys attack, a control system with gantries was installed in December 2015 at Gare du Nord in Paris. Measures were also taken near the entrance of the Channel Tunnel to prevent illegal infiltration of immigrants.

In Nice, the Promenade des Anglais is now heavily defended with reinforced bollards and steel cables.

Standards

Standards exist for cargo land transport. The Transported Asset Protection Association – TAPA – has established Security Standards (FSR/TSR/TACSS) to ensure the safe and secure transportation, storage handling of any TAPA member's assets throughout the world. The Trucking Security Requirements (TSR) represents minimum standards, specifically for transporting products via road within a supply chain. There is also a TAPA TSR certification.

But, when it comes to the selection of private security providers, public stakeholders often award contracts mainly on the basis of cost criteria, not on quality – very similar to aviation and maritime transportation. Enhanced security must however start with the selection of providers that comply with highest quality criteria.

CoESS assist buyers of private security providers in identifying quality criteria with a best value manual entitled "Buying Quality Private Security Services"[29]. The guide has been updated in 2015 in cooperation with UNI Europa and with financial support of the European Commission, in order to be in line with the new EU Public Procurement Directive. For more information about the manual, please refer to **www.securebestvalue.org**

[27] https://ec.europa.eu/transport/sites/transport/files/themes/security/doc/2012-05-31-swd-transport-security.pdf
[28] European Commission (2012). Staff Working Document on Transport Security. Brussels.
[29] http://www.securebestvalue.org

Cooperation between Stakeholders

Cooperation on EU-level

Since the European Commission's Decision 2012/286/EU[30], an expert group on land transport security exists on EU-level (LANDSEC). Its objective is to assist the Commission in formulating and implementing policy initiatives related to land transport security and to foster exchange of best practices among Member States and other stakeholders, including CoESS. It is the only structural cooperation forum on local, national or European level between public and private security services.

Stakeholder cooperation in practice

With regard to train and metro transportation security, the number of stakeholders involved creates the same kind of challenges as in aviation security: we witness a large variety of stakeholders and the security framework of transportation hubs is very complex.

Parts of train and metro stations are completely public, other parts require access control for travellers, and restricted areas are limited to authorised staff. In restricted areas again, there are differences between critical and non-critical areas. Depending on legislation and definitions of such areas, which vary among Member States, different stakeholders are involved in the security framework. Coordination among all involved stakeholders is therefore often challenging, which can lead to significant security gaps.

Cargo transport security by rail or road is a purely private matter, but also here variations in Member States' legislation may have an impact. Legislation varies for example on the possibility to escort vehicles and on the right for private security officers to carry guns.

Gaps and CoESS Experience

Based on evolving risks, legislation, standards and their implementation, PSCs in land transport security have the following concerns that are similar to other transportation modes:

Incident-driven legislation on Member State level

Measures that enhanced security at mass passenger transportation stations on Member State level were introduced in a post-attack climate and are largely reactive. Our concern is that as soon as an attack has taken place, security measures are adopted as a response, and terrorists very quickly change their modus operandi and targets, which has been shown by recent attacks with VaaW.

Countries that have not yet been affected by attacks further often fall short in the introduction of security measures before an incident happens.

Similar to other transportation modes, legislation currently lacks a pro-active response to evolving risks such as CBRN.

---

[30] http://eur-lex.europa.eu/eli/dec/2012/286/oj

Variations in legislation across Member States and missing European guidelines

We assess a lack of an active European approach to the broad and complex area of land transport security and in particular to the security of passenger transport. The increasing frequency of terrorist attacks on mass passenger transportation raises the question whether we need to better secure train stations and transport hubs in general.

Activities of the European Commission in this regard, such as the organisation of stakeholder forums to exchange lessons learned and best practices, have been very helpful. However, in the absence of EU legislation, the competence remains at Member State level and measures are mostly rather taken in a re-active than a pro-active manner.

Especially with regard to international high-speed train connections and the free movement of people, Member States with low levels of security at train stations can become the 'entry point' for security risks. The attack on a Thalys train in 2015 shows that these cross-border networks are attractive targets for terrorist groups and lone wolves.

Security gaps in land cargo

As cargo in the supply chain passes via the road or rail sectors, the absence of common EU rules for supply chain security poses a weakness. Further, past incidents such as the hijacking of a truck prior to the attacks with VaaW in Berlin and Stockholm show that the physical security of drivers and other personnel is at risk due to new threat developments. There is a big untapped potential to reinforce the security of cargo transportation and goods by means of ICT.

Lack of quality criteria in procurement of private security providers

No specific rules exist for public procurement for Critical Infrastructure and land transport, just like it is the case for aviation and maritime transport. As a consequence, contracting authorities often select private security providers on the basis of cost criteria, not on quality of service deliverables.

Liability from acts of terrorism

Another important legislative gap is the inexistence of a harmonised liability regime for the consequences of terrorist attacks. In the event of a terrorist attack, PSCs are not able to face possible third parties' claim, which could relate to amounts exceeding available insurance coverage.

Insufficient coordination and communication among security stakeholders

Similar to aviation and maritime security, the presence of multiple stakeholders in the land transport security setting can lead to insufficient coordination and communication among stakeholders along the security supply chain.

In particular, the legal framework in the Member States does not support the setting up of a two-way open channel of communication for PSCs and relevant law enforcement and/or intelligence authorities. This can create frustration when PSCs provide information to the police, and little or no information is returned, because PSCs don't have a license to receive or handle sensitive information from the police or intelligence services. In order to achieve the objective of effective cooperation, it is important that this issue is addressed.

Insufficient security culture in land transportation

The security supply chain can only be as strong as its weakest link. The lack of a true security culture in the land transportation sector is therefore a major challenge. Security is often perceived by some transport operators to be a negative cost instead of a commodity and service to be provided to passengers like in the aviation sector. Indeed, the return and effectiveness of investments in security is difficult to measure, and there is a clear need to balance passenger facilitation with security. However the frequency of attacks on means of mass passenger transportation can lead to a lack of trust in land transportation.

Future Developments

Public passenger transport

It can be foreseen that means of public mass transportation will remain high-risk and easy targets for terrorist attacks, given the ease of access, as well as dense and constant passenger moves.

While 'conventional' attacks with guns and other types of weapons, as well as explosives, must be reckoned with, we must also anticipate and plan for attacks with CBRN. Our recommendations should be implemented on a risk-based and proportional basis.

Attacks with vehicles as a weapon (VaaW)

Terrorist networks increasingly change their modes operandi as a reaction to enhanced security measures, and the frequency of attacks with VaaW only in the past year makes future similar attacks very likely.

Cargo transport by road

Fierce competition between transport companies, their small profit margins and the idea that insurance companies will cover possible damage can lead to a decrease in investments into cargo and staff protection.

We can also anticipate that there will be more cyber-crime in road transport. Similar to other transportation modes, land cargo becomes increasingly dependent on IT-solutions and computer-based procedures. A cyber-attack on any part of the supply chain can provide criminal networks with access to sensitive information (schedule, cargo worth, routes, plate numbers, etc), leading to severe consequences for land cargo security.

Conclusion and Recommendations

We strongly recommend implementing additional preventive security measures both for passenger transportation and cargo. To support this effort, it is crucial to create a better understanding of security challenges among all involved stakeholders. Further, we call for greater adherence to high-quality procurement standards, and a framework that guarantees a harmonised liability regime for the consequences of terrorist attacks.

Additional preventive security measures

Public passenger transport
Based on the locations and the risk assessment, a different and proportional 'mix' of measures needs to be put in place, which will include security by design, physical security, technology and guarding.

Security by design and / or physical security
For Hostile Vehicle Mitigation, we recommend to use any objects that inhibit vehicles to get close to the area to protect, such as:

→ Concrete blocks;

→ Art that blocks;

→ Gabions;

→ Bollards;

→ Fences.

For hostile person mitigation we recommend enhanced perimeter protection and fences.

Technology and guarding
Additional guarding and surveillance measures have to be based on operational procedures and need to be supported by a CCTV that is controlled from a Control Room that is operated by duly qualified security specialists. Such measures can include:

→ Continuous patrols in departure and arrival zones;

→ Periodical control of lockers and left luggage;

→ Special attention in ticket offices and toilets areas, especially within crowds;

→ Close control of regular station population that may be perceived by the general public as potentially bothersome, or which can be engaged in unlawful activity (e.g. beggars, drug-addicts and well-known pickpockets);

→ Fast intervention in case of arguments or escalations to fights;

→ Access control for sensitive areas of the stations and trains;

→ CCTV and intelligence cameras – we expect fast increase in the number of face recognition and/or detection behaviour cameras;

If the location is under a particularly high threat, X-ray equipment for luggage and Walk Through Metal Detectors can also be used. However these have limitations on passenger facilitation and do not detect non-metal equipment and explosives.

Staff and prevention of insider threats

Procedures for hiring and background checks need to be enforced, especially for staff having access to certain sensitive locations of transportation hubs. Also, we recommend to put in place a safety / security at work policy which enables early detection of insider threats. Regular training / information campaigns can further be of added value to make all staff feel responsible for safety and security. Creating a security culture, not only within the staff of all stakeholder organisations, but also with passengers, is a winning strategy in anticipating both security and safety issues.

Exploiting synergies for more effective security procedures

Synergies exist, and should be fully exploited, between logistics, health and safety and security procedures at transportation hubs. Logistics enable operators to know who/what should be where and when. This is helpful information that can be used as source and baseline to identify security-related irregularities. Limiting access to some areas has benefits from health and safety as well as security perspectives. These are just a couple of examples to highlight the interest of looking for these synergies and making the information smooth and available to those who need it, when they need it.

Road cargo and supply chain security

Regarding cargo transportation security, there are many solutions involving ICTs that can help and reinforce security of goods and personnel. We recommend undertaking the following steps in order to secure the transport from the point of boarding until the point of delivery:

Analysis of the itinerary

Itineraries need to be pre-established by the transport company. In general, these itineraries will preferably include motorways. Frontier points will also impact the itineraries. They should only be changed exceptionally and follow the same basic principles:

➔ Main and alternative itinerary;

➔ Risks:
  • From natural elements (rain, snow, overflow, landslides);
  • From antisocial activities (strikes, demonstrations, attacks).

It is very important to gather relevant information that may affect itineraries (traffic conditions, weather report, analysis of alternative routes) before starting the journey.

The level of security and safety of the itinerary depends on speed (motorways versus secondary roads), lighting, GSM/GPRS coverage, access control on break areas, and frequency of traffic.

Secure parking

Statistics show that the most vulnerable places in road transport are the rest areas, where drivers have to stop in order to comply with legislation. Criminals use this situation to break in the truck and steal merchandise without having use violence against the driver.

The terrorist attack on the Berlin Christmas Market with a hijacked truck shows the urgency of this issue. The vehicle was stationed on an ordinary, remote and not frequented parking lot.

To be secure, parking areas need to meet the following criteria:

→ Sufficient lighting in all infrastructure;

→ Access control;

→ Barriers or closed gates;

→ 24/7 authorised and connected security guards and mobile patrols;

→ Security cameras;

→ Monitoring of pedestrian movements;

→ Pre-booking of parking spaces;

→ Seals control.

We recommend that an authorised person confirms the right placement of seals for the whole truck or container at the first point of departure and at the last point of arrival. Further, taking pictures at the start, arrival and after each stop (as short as it may be) are also recommended practices.

Performance procedure

All types of transport require precise procedures for different situations, and all operating staff must be familiar with them before starting the job and at all stages.

En route procedures should exist for programmed stops; traffic issues and driving through cities; stopping of the vehicle by police; and breakdown.

Procedures also need to exist for certain kinds of incidents such as conventional accidents, fire, roadblock, closed itineraries, as well as attacks, thefts, and assaults.

Permanent monitoring

To protect cargo, the permanent monitoring is highly important. Vehicles should be equipped with geo-satellite devices, which can be monitored in a permanent way from a Control Room with dedicated and specifically trained staff. It is further recommended to also monitor goods from a distance in order to avoid theft, stowaways, and the trafficking of illegal merchandise.

A variety of equipment is available for such purpose, including: locks with GPS-GSM devices; sensors hidden in cargo that allow geolocation at any time; sensor-based light-detecting sensors; and mobile equipment fitted with a panic button that connects drivers with the Control Room for any type of emergency.

Escort of goods

Security escorts, for instance security guards that escort a convoy in a separate vehicle, allow for an immediate reaction capability in case of incident. The role of private security providers is key for such cases.

Here, it is the PSC that provides the planning for itineraries, carries out the original and final control of goods, and deploys its own preventive and reactive procedures.

There is no EU legislation regarding this type of service, and national legislation varies from one Member State to another. This may in certain cases create issues if goods that need to cross borders.

Pro-active EU and national legislation

Legislation on land transport security has always been incident-driven and should become more pro-active, pre-empting and anticipating scenarios including new ways of attacks.

The European Commission's Staff Working Document on Transport[31] from 2012 already identified that EU legislation on land transport security can in some cases be of added value[32].

Standards for the procurement of private security providers

When selecting private security companies to perform missions in any of type environment, cost is not the only criteria of choice. Regretfully, we observe that this is still rarely the case, and quality hardly comes into account for selecting private security providers. There are even cases of procurement (public and private) where the cost of the contract is lower than the collective bargaining minimum salary. As a Social Partner of UNI Europa, and member of the EU Undeclared Work Platform, CoESS feels the need to flag such practices as unacceptable and a clear encouragement to undeclared work.

CoESS and UNI Europa have published a manual – entitled "Buying Quality Private Security Services"[33] with financial support of the European Commission, which guides buyers of private security services through the quality criteria to look for. The guide can be downloaded in 14 languages on www.securebestvalue.org.

Harmonised liability regime for the consequences of terrorist attacks

CoESS calls for a fair and acceptable distribution of responsibilities and risks between the authorities and other parties responsible for security, on the one hand, and PSCs to which security services have been outsourced, on the other hand. Only a clear EU initiative, possibly leading to a common legal framework, or joint strategy by the Member States will be able to efficiently address the issue for all different sectors concerned.

Exchange of information among public and private security stakeholders

Resources dedicated to intelligence need to be reinforced in such a way that attacks can be anticipated and avoided. PSCs can play an important role in this effort as they are usually the first line of response for the most of threats and current modus operandi of terrorists, and intelligence services will not always detect the forthcoming attack.

A clear framework needs to be established for the exchange of relevant information between PSCs and law enforcement / intelligence agencies – bearing in mind data protection and privacy regulatory frameworks.

If the level of threat is heightened, PSCs should be part of the priority stakeholders to inform.

---

[31] https://ec.europa.eu/transport/sites/transport/files/themes/security/doc/2012-05-31-swd-transport-security.pdf
[32] European Commission (2012). Staff Working Document on Transport Security. Brussels.
[33] http://www.securebestvalue.org

Security culture

Smooth cooperation and communication between all stakeholders is a key factor for a successful security policy and operation. If security is to be taken seriously, it can only be within a dynamic process (Plan Do Check Act mode), where security – as well as safety – is considered as a chain, within which each stakeholder knows its own mission, duties, role and responsibilities, understands uses and supports smooth and effective processes. This will promote communication that follows a clear and efficient path so that security can be improved in a constant way.

Seeing security as a service and commodity to passengers while creating a security culture is a winning strategy in anticipating both security and safety issues. For all staff, stakeholders and passengers, the principle of "if you see something, say something" needs to be repeated on a regular basis to keep everyone alert to possible dangers and informed on how and to whom issues should be reported.

Hotlines are being created in a number of countries to this end. In a medium to long term, a single telephone number or application for the whole of the EU could be foreseen, or at least a number that is valid on the same train line even if it crosses borders. In emergency situations, people will act in 'automatic pilot', and for this reasons 'automatisms' need to be created.

Conclusion

All transportation modes, from aviation and maritime to land, are increasingly vulnerable to intentional unlawful acts against transportation networks, businesses, and the public. They face very similar threat environments and developments: from conventional and insider threats to more sophisticated attacks including HMEs, cyber, drones, VaaW, and CBRN. The recent series of attacks in Nice (2015), Brussels (2016), Berlin (2016), Stockholm (2017), London (2017), and Barcelona (2017) sadly confirms this development and raises the question of how well we are prepared to prevent future attacks.

European legislative frameworks of aviation, maritime, and land transportation security vary widely – from the highly regulated aviation sector, to land transport where no EU legislation exists. Variations remain in legislation, standards, and their implementation among Member States. But, all transportation modes face very similar threat environments, show comparable loopholes in the security supply chain and can learn from each other.

Therefore, policies and security measures that address these weaknesses need to be more preventive in order to pre-empt attacks from the start. This can be achieved by stricter security measures at transportation hubs, following for instance best practices in aviation security. But it is highly important to introduce such measures independently from past attacks and an environment where quick action is needed, but rather based on distinct security risk assessments in each transportation mode to assure support of all parties involved. This report provides recommendations on suitable measures that should be introduced in each transportation mode, based on identified risks.

Many improvements can also be made on the human level. This starts with the personnel responsible for transportation security. Employees must be properly trained and informed about how to deal with current and evolving threats. The lack of standards or their insufficient implementation is a severe loophole in security frameworks.

Another important way to improve transportation security is the introduction of public procurement quality guidelines for the contracting of PSCs. Too often, security providers are chosen based on price-criteria only. CoESS supports procurers in identifying quality criteria, mainly by providing a best value manual entitled "Buying Quality Private Security Services"[34]. The guide can be downloaded on **www.securebestvalue.org**.

Further, better cooperation and exchange of information across the large variety of stakeholders involved in security supply chains and the operation of transportation hubs is crucial. PSCs are an important partner in this effort. They bring hands-on experience as first in-line responders to incidents and represent a valuable source of information and partner in the set-up of security plans. However, PSCs are currently not even able to face possible third parties' claim in the event of an incident, which could relate to amounts exceeding available insurance coverage. Here, we need a coherent liability regime.

Creating a security culture across stakeholder organisations and the wider public is a winning strategy to help anticipate both security and safety issues. It is fundamental that all stakeholders have a proper knowledge of the kinds of threats they are dealing with and have the best tools at hand to prevent future incidents.

---

[34] http://www.securebestvalue.org

CoESS

Acting as the voice of the **security industry**

coess.org

Jan Bogemansstraat | rue Jan Bogemans 249
B-1780 Wemmel
Belgium
chantal@coess.eu

T +32 2 462 07 76
F +32 2 460 14 31