Assessment of the European Programme for Critical Infrastructure Protection in the surface transport sector

Ralf Hedel*

Department of Strategy and Optimization,
Fraunhofer Institute for Transportation and
Infrastructure Systems (Fraunhofer IVI),
Zeunerstraβe 38, 01069 Dresden, Germany
Email: ralf.hedel@ivi.fraunhofer.de
*Corresponding author

George Boustras

Centre of Excellence in Risk and Decision Science (CERIDES),
Ioannis Gregoriou School of Business Administration,
European University Cyprus,
6, Diogenis Str., 2404 Engom, Nicosia, 1516, Cyprus
Email: G.Boustras@euc.ac.cy

Ilias Gkotsis

Center for Security Studies (KEMEA),
4, P. Kanellopoulou Str.,
Athens GR-101 77, Greece
Email: i.gkotsis@kemea-research.gr

Ioanna Vasiliadou

Aegean Motorway S.A.,
Moschochori, 441500 Larissa, Greece
Email: ivasileiadou@aegeanmotorway.gr

Paul Rathke

Department of Strategy and Optimization,
Fraunhofer Institute for Transportation and
Infrastructure Systems (Fraunhofer IVI),
Zeunerstraβe 38, 01069 Dresden, Germany
Email: paul.rathke@ivi.fraunhofer.de

Abstract: In the course of emerging threats of the 21st century, this paper aims at supporting the further development of the European Programme for Critical Infrastructure Protection (EPCIP), in particular the directive 2008/114/EC on designation and protection of European Critical Infrastructures. It provides a comprehensive review of this legal framework by compiling experiences of practitioners collected during the European Surface Transport Operator (EUSTO) forum and a series of semi-structured expert interviews. The answers of the EUSTO participants assess how the single elements and approaches of the EPCIP have affected their work. Furthermore, the review identifies the challenges that need to be addressed in the future. The third part of this paper provides a guideline on setting up an Operator Security Plan, which is specifically required by the directive. The template could initiate European harmonisation of security plans, contributing to the improvement of EPCIP.

Keywords: critical infrastructures; critical infrastructures protection; transport infrastructures; surface transport; European Union; EPCIP; directive 2008/114/EC; Operator Security Plan; OSP; terroristic threats; criminal threats; resilience; practitioners.

Reference to this paper should be made as follows: Hedel, R., Boustras, G., Gkotsis, I., Vasiliadou, I. and Rathke, P. (2018) 'Assessment of the European Programme for Critical Infrastructure Protection in the surface transport sector', *Int. J. Critical Infrastructures*, Vol. 14, No. 4, pp.311–335.

Biographical notes: Ralf Hedel graduated in Business and Social Geography (minor in computer sciences and thematic cartography) and worked in transport research at the DLR (German Aerospace Center) and in the consultancy, Probst & Cons for several years. In parallel, he accomplished his PhD thesis in the topic of decision support for the evaluation of development strategies in transport networks. Since 2012, he has been working at the Fraunhofer IVI, Department of Strategy and Optimization. He supported the coordination of the EU-project IDIRA (interoperability of data and procedures in large-scale multinational disaster response actions), led the institute's activities within IMPRESS on preparedness and response of health services in major crises and currently manages the contribution to EU-CIRCLE on critical infrastructure resilience at the Fraunhofer IVI. He is the Chair of the ECTRI Thematic Group Security and Risk Analysis.

George Boustras is a PhD in Probabilistic Risk Assessment from the CFES at the Kingston University, London. He is currently a Professor at the European University Cyprus (EUC) and Director of the Center for Risk and Decision Sciences (CERIDES). He sits at the Management Committee of Secure Societies – protecting freedom and security of Europe and its citizens of 'HORIZON 2020'. He is the Editor-in-Chief of *Safety Science* (Elsevier) and member of the Editorial Board of *Fire Technology* (Springer), the *International Journal of Emergency Management* and *International Journal of Critical Infrastructure* (both Inderscience).

Ilias Gkotsis is a Mechanical and Aeronautics Engineer with an MSc in Energy Production and Management. For several years, he has worked in transport research projects and studies (traffic modelling and analysis, transport management, traffic emissions and environmental assessment, etc.) at the Department of Transportation Planning and Engineering, NTUA, where he is currently completing his PhD thesis. Since 2012, he has been a Research Associate of the Center for Security Studies (KEMEA), where he is also heavily involved (implementation, management and coordination) in EU and nationally funded R&D projects, regarding security, crisis management, critical

infrastructure protection, border surveillance, civil protection, etc. Finally, he supported the coordination of EUSTO activities and was responsible for the template of an operator security plan.

Ioanna Vasiliadou is a Transport Engineer with expertise in business administration. She has 20 years of experience in the field of transport engineering, strategic planning, critical infrastructure protection, safety analysis, transport infrastructure and civil protection and relevant research topics. She has participated in a significant number of European research projects and has worked for large motorway construction and operation companies, as well as for the transport division of the Organising Committee for the 2004 Olympic Games. From 2013 to 2016, she was a Research Associate at the Center for Security Studies (KEMEA), where she coordinated EUSTO among several other security projects. Currently, she is the Head of Traffic Analysis and Road Safety in Aegean Motorway S.A.

Paul Rathke is a student of Transportation Engineering at the Technische Universtität Dresden (Dresden University of Technology). Simultaneously, he is a student associate at the Fraunhofer IVI, involved in projects related to critical infrastructure resilience.

1 Introduction

1.1 Context – the EUSTO project

In a globalised and highly interdependent world, logistic and transportation networks are significantly important and vulnerable at the same time. Emergencies arising from terrorist threats, like the recent incidents in Paris, Brussels and London highlight the need for transport security managers to minimise the vulnerability of their critical infrastructure (CI) assets, such as infrastructure, equipment and personnel. According to the respective governments, transportation systems remain key targets for terrorist and extremist groups due to the potentially high impact on a social, economic, psychological and political level.

Under these circumstances, effective and sufficient measures to protect transport infrastructures are essential. In the course of ongoing globalisation, CI protection is a cross-border issue. On a European level, the European Surface Transport Operator (EUSTO) project has thoroughly reviewed the existing regulations of the European Programme for Critical Infrastructure Protection (EPCIP) through the interaction and collaboration with relevant stakeholders, practitioners and researchers.

The results of the conducted surveys and workshops provide specific information on the potential for further developing the EPCIP. In particular, this article focuses on the directive 2008/114/EC, the major element of the program. Chapter 2 precisely assesses the effectiveness and implementation of this directive. In terms of viable suggestions for the improvement of risk management (RM), participants of the EUSTO forums supported the development of an Operator Security Plan (OSP) template, as described in Chapter 3.

These elements of CI protection can be better understood in the context of the risks that land surface transportation faces. Hence, Section 1.2 depicts different types of such emerging threats in the 21st century.

1.2 Emerging threats in transportation

Mass transportation systems hold a unique position as potential targets for attacks. They are built up as networks and feature a large concentration of people as well as a fundamental economic role. In course of the emergence of vehicle-to-everything (V2X) communications, mass transit systems have become even more vulnerable, particularly to physical and cyber security threats. Moreover, increased security levels in air transport caused attackers to refocus on surface transport terrorism.

Despite the awareness of the problem among stakeholders, land transportation systems remain highly vulnerable for certain reasons. Essentially, they are designed to provide fast and cheap transport. The required speed imposes certain limitations to the extent and existence of security checks, whereas the required (low) price limits the sophistication of the security checks and technologies employed.

Security in transportation systems concerns the detection, identification, mitigation and protection against physical and cyber-physical threats towards users and the infrastructure. "Transportation security, namely the identification, assessment, and reduction of vulnerabilities within and threats to the vast transportation network, has expanded greatly, experiencing great change and challenge along the way" (Bullock et al., 2017).

1.2.1 Definition of risk and threat models in the directive 2008/114/EC

In general, risk is defined as 'effect of uncertainty on objectives' (ISO, 2009) and is linked to potential events and consequences. The standard states: "Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence" (ISO, 2009). The directive 2008/114/EC addresses the protection of transport infrastructure in the abovementioned context of emerging threats. Risk analysis and RM are the essential parts of the directive.

However, potentially critical events or threats are not specifically defined in the directive. They differ between distinct categories of CIs and among different member states of the European Union. Paragraph 6 of the directive underlines that "the primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures" (European Commission, 2008). Despite this absence of definite threat models, threat analysis is explicitly mentioned as part of the step to identify European Critical Infrastructure (ECI).

1.2.2 Motivation of attackers

Risk analysis should consider different types of attackers and their motivations. Extensive knowledge on the intentions behind attacks exists for cyber-security threats (Han and Dongre, 2014). Most studies focus on certain groups of attackers, distinguished by their relation to an organisation (insiders or outsiders) as well as their level of experience and skills. These professional levels range from amateurs to hackers and finally, professionally organised groups. Cohen et al. (1998) even distinguishes 35 different types of cyber attackers. The motivation behind their actions can be generally categorised according to the following three dimensions (Gandhi et al., 2011):

- Political dimension: politically motivated attackers can be part of activist's or extremist groups protesting against certain policies or political action. On a national level, this dimension covers warfare and international espionage. It can also include terrorist groups that use violence to spread their propaganda.
- Socio-cultural dimension: conflicts between different social groups or ethnic groups can be a major motivation behind attacks on CI. They often refer to a conflict on power, resources and control, attributes that transport infrastructure provides to a large extent.
- Financial dimension: the intention of economic benefit is widespread, especially among organised cyber attackers. Due to their importance, transport CI can be very attractive to these groups, especially for blackmail.

Attacks that do not fit into any of these dimensions are usually carried out by individuals that follow individual incentives, e.g., personal satisfaction, adventure/fun, retaliation (e.g., against a former employee) (Han and Dongre, 2014).

1.2.3 Types of threats

As stated in Section 1.2.1, the directive does not specify categories of threats to surface transport. However, the public has recently paid high attention to the following threats:

- cyber threats
- physical threats
- chemical, biological, radioactive and nuclear threats (CBRN)

Cyber threats

The operation of transport networks is largely digitised. As more devices and control systems are connected online, more vulnerabilities appear, increasing the potential for the disruption of physical assets. Advances in technology and telecommunication have even resulted in new modes of electronic warfare (Colarik and Janczewski, 2015).

From a technological point of view, cyber-security threats emanate from the emergence of V2X communication in transport. It is part of intelligent transportation systems and requires a communication partner for the respective vehicle. This can be either another vehicle (V2V) or a part of infrastructure (V2I) (Weiβ, 2011). Although V2X cooperation can bring about important benefits, its security constitutes a significant challenge. The higher the number of internal and external partners, the higher the risk of cyber-related vulnerabilities. Possible areas of intervention by unauthorised users are navigational sensors and controllers, both sensitive parts of a common control circuit for V2X (Naeem, 2012).

Moreover, intelligent transport infrastructures (e.g., smart motorways, railway systems) rely on supervisory control and data acquisition (SCADA) systems. Alcaraz et al. (2008) have pointed out that increasing interdependency of SCADA systems with other networks can lead to dreadful cascading effects when being attacked. Thus, the authors propose high frequencies of security analyses. Cai et al. (2008) emphasised the

necessity for special measures to be undertaken to ensure SCADA security. They have shown the differences of original IT networks compared to SCADA revealing significant vulnerabilities, e.g., the use of old protocols or the conflict of anti-virus software and real-time processing of SCADA data.

In general, the authors of this paper consider the following potential consequences of cyber-attacks in transportation:

- impacts on operations resulting in delays
- injuries or casualties resulting in social, economic and political loss
- impacts on freight, rolling stock or infrastructure assets resulting in financial loss and loss of credibility
- data loss resulting in financial loss and loss of credibility.

The two incidents described hereafter illustrate the danger of cyber-threats in transportation.

In 2008, a teenager took control of the tram system in Lodz, Poland, causing four train derails. As described above, V2X communication systems introduce a number of uncertainties into the system. Based on the published police reports, the system was compromised easily and fortunately did not lead to any casualties (Baker, 2008).

A similar incident occurred in South Korea between March and August 2014. Almost 60 computers belonging to subway employees were infected by malware similar to a type that North Korea had used in the past, but the company stressed that the hack did only leak data and information and did not affect operations (AFP, 2015).

Physical threats

Physical security threats directly affect users, infrastructure or operations and include terrorist attacks, natural disasters, theft of valuable cargo, crime in public transport and the movement of hazardous materials. A database provided by the Mineta Transportation Institute's National Transportation Security Center (MTI/NTSC) provides information on attacks on public surface transport since 1970 globally (Jenkins et al., 2010).

According to analysts at the Center for Nonproliferation Studies and from the perspective of WMD terrorism studies (Dolnik and Pate, 2002), the year 2001 was unprecedented. The mass-casualty terrorist attacks of 11 September 2001, demonstrated a willingness of some terrorists to kill large numbers of people indiscriminately to achieve their objectives. The high number of passengers in surface transportation fits to the strategies of these attackers.

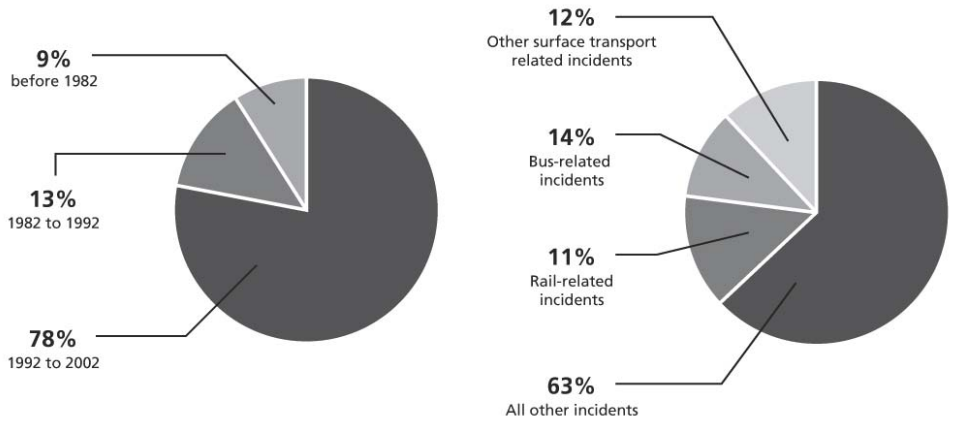
In Europe, the London bombings in the year 2005 are an example of the dramatic impacts that physical attacks can have. In a series of coordinated suicide bomb attacks in central London, attackers targeted civilians using public transport. Four Islamist extremists separately detonated three bombs in quick succession aboard underground trains across the city and later added a fourth on a double decker bus. Fifty-two civilians were killed and over 700 more injured (CNN Library, 2017).

More recently, the 2016 attack on Maelbeek metro station in Brussels has once more shown the impact of physical attacks on public surface transport services. The explosion caused by a bomb detonated in the middle carriage left 16 people dead (BBC, 2016).

CBRN threats

Since 1900, there have been more than 100 confirmed attacks using chemical and biological agents that caused casualties (Monterey WMD Terrorism Database, http://wmddb.miis.edu/). The 1995 Aum Shinrikyo Sarin gas release in the Tokyo subway was perhaps the most serious. The incident resulted in 14 total fatalities, more than 100 cases of chemical poisoning and 1,000 cases of mild contamination. About 4,500 victims required decontamination for psychological, rather than physical, reasons (Olson, 1999). Since the mid-1990s, however, the threatened use of chemical and biological agents has increased, tripling in number. As indicated in Figure 1, the number of incidents related to chemical and biological weapons increased rapidly, in particular in 2001.

Figure 1 CBRN attacks by (a) time period and (b) sector



(a) (b)

Source: After Dolnik and Pate (2002)

Considering a statement of the former French Prime Minister, Mr. Manuel Valls in the aftermath of the 13 November 2015 attacks in Paris that France could rule out a chemical attack, CBRN threats are still relevant for transportation security (New York Times, 2015).

The European Commission identifies CBRN risk mitigation and identification as a top priority in its agenda. As stated in a press release of 2014, it aims to increase awareness and knowledge concerning CBRN threats as well as to improve cooperation with research institutes and other security stakeholders (European Commission, 2014).

2 Review of the directive 2008/114/EC and the EPCIP

2.1 Purpose: review of the directive

The EPCIP "establishes a procedure for identifying and designating European Critical Infrastructure (ECI) and a common approach for assessing the need to improve the protection" (European Commission, 2017).

The rules of the directive 2008/114/EC require a review that the EUSTO consortium contributed to by providing recommendations for its further development. This chapter aims at presenting and discussing statements of stakeholders during the EUSTO forums. It is subdivided into two sections. The first part introduces the objectives, history and instruments of the EPCIP that will be assessed and summarised within the second part.

2.2 EPCIP overview

2.2.1 History and objectives of EPCIP

Europe has a long-standing history of approaches to improve CI protection. Past terrorist attacks fostered the development and adoption of the EPCIP. Some milestones of its development are:

- 2004: proposal of the EPCIP and the Critical Infrastructure Warning Information Network (CIWIN) (European Commission, 2004)
- 2005: adoption of the green paper on ECIP (European Commission, 2006)
- 2008: adoption of the directive 2008/114/EC, the main instrument of the EPCIP (European Commission, 2008).

The EPCIP comprises the following pillars (European Commission, 2006):

- means for its implementation (e.g., EPCIP action plan, CIWIN)
- support for member states concerning National CIP
- contingency planning
- external dimension (exchange of information with non-EU countries)
- EU security research program on "prevention, preparedness and consequence management of terrorism and other security related risks"
- financial measures.

For an extensive description of the history of EPCIP approaches, please refer to Lazari (2014) and the European Commission (2012).

2.2.2 Directive 2008/114/EC – the main instrument of the EPCIP

The directive 2008/114/EC functions as the main instrument of the EPCIP. Firstly, it provides definitions of CIs and ECIs. According to the directive, ECIs are: "Assets, systems or parts thereof located in EU member states which are essential for vital societal functions […] the disruption or destruction of which would have a significant impact on at least two EU member states" (European Commission, 2008). The directive provides concrete support for three phases of EPCIP.

The *phase of identification* includes specific criteria to identify CIs:

- sectoral criteria
- CI definition

- transboundary elements
- cross-cutting criteria.

The *phase of designation* includes all steps to negotiate and to decide on the criticality of any specific infrastructure:

- notification of affected member states
- bilateral discussions and agreements
- final decision by the 'hosting country'.

Finally, it provides two instruments that really contribute to the protection of infrastructures:

- OSP (obligatory unless similar regulations are in place)
- liaison officer as contact point between the ECI owner/operator and relevant member state authorities.

2.2.3 State of implementation of the directive 2008/114/EC

Lazari (2014) provides an overview on transposition into national regulations, respectively regulatory frameworks. In 2011, most of the member states had completed this process. However, the actual implementation varies considerably among them (Lazari, 2014).

Although no ECI has been designated among the EUSTO participants, most of the surface transport operators/owners have already progressed in the development of an OSP for their infrastructures.

2.2.4 Review initiatives

The directive 2008/114/EC was adopted on 8 December 2008. Giannopoulos and Schimmer (2011) describe the course of workshops on its implementation between June 2009 and December 2011. In line with the directive, the review process started on 12 January 2012. Several initiatives were established to assess the status of implementation as well as to contribute recommendations for its further development.

The European Commission (2013) provided an update concerning the single elements of the EPCIP, consisting of a pilot phase with four selected CIs (EUROCONTROL, Galileo, Electricity Transmission Grid and European Gas Transmission Network). Based on that experience, the EPCIP will be further developed in the following directions:

- strengthen risk mitigation, preparedness and response measures
- foster cooperation
- provide funds for the implementation of large and strategic cross-border projects
- facilitate CIP policy development.

2.3 Assessment of EPCIP's current status and recommendations for further development

2.3.1 Working methodology

In the framework of the EUSTO project, two questionnaires were developed and distributed in order to obtain the required information in a structured way. The first questionnaire aimed at generating knowledge about the implementation of the directive 2008/114/EC. It was sent to the national contact points (NCPs) of all 28 member states twice. Twelve NCPs replied and returned useful information. However, even these few respondents revealed important information. The second questionnaire provided more detailed insights concerning the knowledge, perception, effectiveness and suggestions regarding all EPCIP elements. The most relevant questions of the first questionnaire were integrated again in order to achieve a broader knowledge and increase representativeness. During the third EUSTO workshop in Cyprus (December, 2015), the participants discussed the second questionnaire with the audience. Around ten questionnaires were returned and analysed.

The consortium conceded the interviewees a high level of confidentiality; therefore, this publication does not disclose any information that allows conclusions on a specific country, infrastructure or operator.

2.3.2 Knowledge and awareness of EPCIP elements

During the EUSTO project, participants were asked about their knowledge on the EPCIP and its elements: the CIWIN system, research projects, NCPs, expert groups, respective stakeholder dialogue platforms and financial support for member states.

Most respondents know at least one of its elements, especially the directive 2008/114/EC and NCPs. The publicity of other elements, however, varies. Surprisingly, financial support, expert groups/stakeholder dialogue platforms and research projects suffer from low publicity. Even taking into account that the survey is not completely representative for all of Europe, the reasons for such low levels of awareness remain unclear.

Research projects, expert groups and various stakeholder dialogue platforms have already spent considerable efforts on dissemination, e.g., by newsletters, websites or public events. Nevertheless, operators/owners, which are not yet recipients of – or even participants in such activities, are neither obliged to nor capable of informing themselves regularly about European developments. Research and dialogue initiatives create their own registries of only a few interested practitioners. A common database of stakeholders would increase the efficiency of public relations efforts. It should be jointly prepared by the NCPs and include transport providers and authorities, infrastructure operators and major security companies.

One regular newsletter sent out to registered stakeholders summarising the latest information on new regulations, emerging threats, research results and events could gain much more attention than many individual e-mails. Since language barriers may be an obstacle for some stakeholders, such information should be available in different languages of the EU. Furthermore, relevant associations, like the International Association of Public Transport (UITP), could be integrated into this dissemination process.

2.3.3 General influence of EPCIP elements

Another important question of the survey considered the influence of the EPCIP elements on operations within the organisations. According to the answers, the directive 2008/114/EC and the NCPs have firmly influenced the stakeholders. The influence was stronger in countries with lesser developed national protection approaches than in countries with mature protection programs, supporting the thesis of the European Commission (2012).

Expert groups and stakeholder dialogue platforms were assessed as significantly influencing the work. However, they are not well-known. This emphasises the necessity that expert groups/stakeholder dialogue platforms increase their publicity.

2.3.4 Assessment and further development directions

EUSTO asked whether the main elements within the directive 2008/114/EC provide successful support for the work of the respective stakeholder.

Phase 1: identification of potential ECIs

In the phase of CI identification, the directive provides the following elements, all of them assessed as supportive:

- definitions of CIs, ECIs and other terminology
- criteria for the classification of CIs (‘sectoral criteria’, ‘cross-cutting criteria’ and ‘transboundary criteria’).

Most countries have identified none or only a few transport infrastructures as potential ECIs and no transport infrastructure has conclusively been designated as ECI. Interviewees have repeated the fact that infrastructure owners/operators and administrations fear additional workload and costs as well as the obligation to share information once an infrastructure is classified as critical. Another frequently repeated explanation was that the respective infrastructures are considered to be sufficiently protected by the national framework. The European Commission (2012) explains that many countries started the identification of CIs by analysing existing national registries of CIs, which are based on national impact considerations. This way, cross-border impacts are probably ignored systematically.

On the one hand, the transport network is redundant in most cases and provides alternative routes and modes [European Commission, (2012), p.9]. Thus, following the quantitative approach of the directive, transport infrastructure is not critical. On the other hand, it is sometimes (qualitatively) argued that a disruption of infrastructures, e.g., international rail freight yards, central railway stations or European motorways, could cause severe ramifications in economy and society, even to multiple countries. Both argumentations are based on ex-ante considerations where the first argumentation is apparently stronger than the second one.

Therefore, the impact criteria should be extended to include interdependencies between other sectors (e.g., cascading economic impacts on production due to disruption of supply chains). The extension from impact assessment to risk assessment explicitly integrates probable disruptions in the considerations. Many transport operators already conduct risk assessments. However, a broadly accepted framework and viable,

harmonised guidelines for the identification, assessment and management of risks are required.

Phase 2: approach for the designation of ECIs

The EUSTO consortium asked to assess the main elements for the designation of ECIs:

- obligation to notify other affected member states about identified ECI
- bilateral communication and agreements with affected member states
- annual review on criticality by the hosting country.

The majority of the respondents assessed these elements as 'successful'. However, the EUSTO team received critical comments as well. A common point of criticism is that bilateral communication between member states is often not satisfying. Some member states tend to minimise the information shared. Moreover, it can be questioned whether the final decision should be exclusively up to the hosting country, although other countries might be even more affected by a disruption. An updated directive should facilitate and encourage multinational cooperation. In case of contradictory opinions about the criticality, a commission consisting of the affected EU member states could solve conflicts in a collaborative manner.

Phase 3: protection of ECIs

The main obligations explained by the directive 2008/114/EC are:

- promotion of risk analysis
- setup of an OSP
- designation of security liaison officers for all ECIs.

These elements received the highest affirmation by the interviewees and are already part of national security plans for almost every CI. Nevertheless, the current state of funding for security efforts, which increases with the number of designated ECIs, was criticised.

The further items of the directive 2008/114/EC were assessed to be successful without any specific comments:

- obligation to share generalised information on ECIs with the European Commission
- support by the commission to share best practice and support training
- installation of NCPs.

By 2012, all member states had appointed an NCP (European Commission, 2012) and workshops on the implementation of the directive had been held (Giannopoulos and Schimmer, 2011).

According to the interviewees, the most serious threats are terroristic, intentionally destructive attacks and natural disasters. As the directive follows an all-hazard approach, it is regarded as a proper way to address these threats.

2.3.5 Challenges and high priority measures

The results of the EUSTO questionnaire revealed that the most serious challenges for the implementation of the directive 2008/114/EC in the respective countries are:

- lack of adequate resources
- political interference
- lack of adequate national legislation.

The explicit priorities for improvement are:

- financial support
- exchange of operational information and of best practice examples
- research.

The implementation of measures related to risk assessment and risk mitigation is a matter of financial resources. For example, authorities require CCTV systems in many transport regions, whereas these systems are paid and maintained by transport operators only. Moreover, they have to setup and regularly update plans. These circumstances reduce the ability and motivation of operators to introduce further security technologies and to designate infrastructures as critical. Hence, responsible stakeholders need adequate compensation for their additional efforts enabling them to protect designated ECIs. European or national directives could define minimum standards on hard and soft security measures together with clear statements on their financing.

Exchange of operational information apparently takes place within small groups of a few stakeholders (e.g., within one public transport association) only, but not in a structured way across the barriers of organisations and countries. A way to address this fact would be to develop a central/hierarchical system for fully organised operational information exchange. Such a system should involve authorities as well as operators and include alerting functionalities. Therefore, mutual trust, cooperation and communication within and beyond organisations are key factors to be improved. Especially, the international sharing of information about incidents and threats remains unsatisfying.

Up until now, the way in which CIP is addressed differs considerably between member states. Mutual exchange helps to identify and disseminate knowledge on best practices. Transport operators and infrastructure operators require a competent single contact point within the responsible authority to discuss and coordinate all the security measures. In the future, common European standards and procedures could be developed and introduced. Considering the varying conditions and necessities of CI operators and EU member states, there is no uniform solution though. The EPCIP should provide possibilities for an individual implementation.

In this context, the potential growth of the spatial dimension of threats has to be considered. The EPCIP addresses this through the ‘external dimension’. Cooperation with countries outside the EU, e.g., the Middle East, should be continued and expanded.

The exchange on best practices, e.g., security plan templates, is effective, but existing exchange initiatives should be orchestrated to improve their effectiveness. The variety of existing web tools makes it cumbersome to collect information or to decide which event is worth attending. Taking into account experiences of the EUSTO project, exchange

among practitioners requires awareness, trust and time. Therefore, such exchange initiatives should last at least three years.

Another focus should be on the security staff, especially their education level, training, equipment and security assessment. Multiple times, interviewees demanded for trainings and exercises to be part of the directive, including guidelines on their frequency (scope and content depend on the country and current threats). They could be developed together with transport associations.

The survey participants also assessed a cultural change among transport system users and staff as necessary. Public awareness campaigns raising sensitivity and appreciation for security staff and security efforts in general could be integrated in the prospective EPCIP.

In order to improve the field of research, roadmaps as developed, e.g., by creating an agenda for research on transportation security (CARONTE) project should be considered in funding decisions. Participants of the EUSTO international conference identified the following topics:

- role of social media
- disaster impact on transport operator staff (focus on day one after an incident)
- passenger behaviour in case of an incident and evacuation process.

Research initiatives and their results should also be disseminated to a wider audience. Moreover, the transparency of risk assessment methodologies is low. Common methodologies together with IT-based tools could be developed and introduced further.

3 A reference OSP – a non-binding guidebook for practitioners

3.1 Context and purpose of the reference OSP

The directive 2008/114/EC requires member states to ensure that an OSP or an equivalent measure is in place for each designated ECI. The purpose of the OSP process is the identification of ECI's critical assets and already existing security solutions for their protection.

EUSTO built common guidelines for developing OSPs for surface transport CI with an EU dimension based on best practice, in pursue of the objectives of the directive 2008/114/EC. The reference OSP is a non-binding guidebook for surface transport operators. This template describes the process and key concepts, while accompanying and supporting the CI security manager in the development of a specific OSP.

In order to produce this template, the EUSTO consortium has used the active involvement of NCPs and surface transport stakeholders through discussions and personal interviews. This knowledge has been combined with the contributions of EUSTO partners in workshops and the EUSTO online forum. A dedicated discussion and information gathering has been achieved during the 3rd EUSTO Forum.

3.2 Operation security plan development process

3.2.1 Identification of the CI

This section defines the external and organisational environment in which the security plan has to achieve its objectives. Identifying this environment before the risk assessment phase ensures that the OSP receives the necessary support from key stakeholders and reflects on important strategic factors that require its preparation or review.

Standards

The first phase relates to the identification of core components of international, EU and national regulation frameworks, protection strategies, laws and directives. The objective of the materials is to familiarise users with the 'preparedness architecture'.

Methodology on a national basis

The CI operator should follow national RM methodology or develop one in order to identify and manage the risks that their critical services are exposed to. Any of the methodologies followed or developed should consider the following sequence.

Figure 2 Important steps of RM development

A fundamental aspect of RM methodologies is that the used values and estimated parameters (vulnerability, impact, etc.) are repeatable and comparable over time. Methodologies such as this help organisations to establish priorities and to focus on security resources, thus reducing risk exposure. Once the context (cause, scope, organisation, methodology, assessment criteria of the RM process) is known, the risk assessment phase is carried out based on the chosen methodology.

CI profile

An initial stage before the risk assessment is to shape the CI profile through the identification of the most important assets in the organisation, subsequently selecting these in turn for application of the full security management plan process. After the selection of an asset, its critical processes, components and dependencies have to be analysed.

Hence, the first part of the asset characterisation process is to identify and rank all corporate assets regarding their overall importance to the organisation and the wider community. This ensures that requirements of critical assets are addressed first, thus supporting the cost-effective and targeted allocation of resources. Once an asset has been classified as being critical, the stakeholder should identify threats and select risk-reducing countermeasures.

The second part of the asset characterisation process is to achieve a more detailed understanding of the asset, thereby identifying relevant factors to subsequent phases of the assessment process. It also includes the determination of the asset's critical parts that require special consideration.

The CI profile should provide a description of assets and facilities, distinguishing between infrastructure, personnel and equipment.

3.2.2 Risk assessment

The implementation of an effective OSP requires an understanding of events that could state a threat to personnel, operations, and information. Assessing and categorising the consequences of these events is the basic function of a RM process. The assessment of CI risks helps the security manager to determine whether the countermeasures in place are adequate or additional measures must be implemented.

This process includes the collection of information and the assignment of values to risks for the purpose of informing priorities, developing or comparing courses of action and informing decision making. Factors such as the likelihood of an undesirable event and its consequence(s) can be quantified afterwards. Therefore, effective risk assessment requires timely and reliable information regarding threats. The actual method of determining and quantifying risk is dictated by the organisation performing the assessment.

Threat assessment

A threat assessment comprises the identification of entities, actions and occurrences that can (potentially) harm or destroy critical assets. It considers all possible threats (e.g., natural, terroristic or accidental) for a given facility/location. Threat data can be derived from various resources including security organisations, intelligence community reports and authorities.

There are a variety of threats and resources to consider when conducting a threat assessment. For natural hazards, historical data and future trend analyses concerning the frequency of occurrence effectively determine the likelihood of the given threat. For criminal threats, the crime rates in the surrounding area provide a good indicator. In addition, the type of asset housed in the facility may also increase the attractiveness for an aggressor. They are also directly related to the likelihood of various types of accidents. For example, a facility using heavy industrial machinery will be at higher risk for serious or life-threatening job-related accidents than a typical office building. For terrorist threats, the symbolic value of the facility as a target is a primary consideration.

Vulnerability assessment

The assessment of threats is subsequently followed by a vulnerability assessment. This process includes the identification of physical or operational features that may render an entity, asset, system or network susceptible or exposed to hazards. Existing countermeasures must be compared to those stipulated by the baseline level of service to determine existing deficiencies. The lack of appropriate and effective countermeasures equates to vulnerability. Site-specific vulnerability assessment data must be protected in accordance with appropriate agency guidance.

Consequence assessment

The consequence assessment analyses actual effects of an event or incident using developed threat scenarios. The assessment process itself considers how each threat scenario may impact each of the critical assets identified in Section 3.2.1, respectively the CI as a whole. It subsequently takes into account type and severity of the resulting consequences.

Interdependencies

The scope of the OSP covers one specific surface transport CI. However, interdependencies between its suppliers and business partners cannot be ignored. Surface transport infrastructures are interconnected with other sectors such as ICT and Energy. An event or threat to another sector's CI may have a cascading effect, which finally affects surface transport. The identification of interdependencies improves the evaluation of weak points, threats or risks. Hence, geographical or sectorial interdependencies must be identified and analysed. The collected results of these assessments can be used to adapt the prioritisation of resources.

3.2.3 Development of the security plan

Establish priorities and responsibilities

Plan development starts with identifying the purpose of the document. Although the plan should be flexible enough to cover a broad range of security incidents, the use of a prioritised scenario-based list of critical event types ensures its effectiveness. This list should consist of events most likely to occur, as well as those with far-reaching consequences. Moreover, establishing priorities has four main objectives. It should clarify:

- the purpose of the OSP
- situations that require the use of an OSP
- limitations of operations
- the context of the OSP within existing security and emergency plans.

As part of this phase, key personnel and their responsibilities are determined. Priority security tasks should be listed and assigned to a specific individual known as the primary or principal. Secondary responsibility should be assigned to other individuals whose ability to perform will not be compromised by the loss of the primary. Interdependencies of functions should be delineated between departments and coordinating points established to facilitate liaison in areas of overlapping responsibility. This section of the plan has to provide clear and concise direction to assigned personnel regarding their primary and secondary duties. The goal is to achieve the stated objectives and security requirements of the plan under all potential operating conditions or scenarios. Therefore, developing an organisational structure is the key objective of this part in the OSP. This structure should contain a clearly defined chain of command, designated roles and responsibilities, structured as the following:

1 Responsibilities

2 Continuity of service
   - designating lines of succession and delegating authority for the successors
   - developing procedures for relocating essential departments
   - developing procedures for essential personnel, equipment and supplies
   - establishing procedures for backup and recovery of computer and paper records.

3 Contact information

3.2.4 Strategies and countermeasures

Consistent with emergency management principles, risk and vulnerabilities, reduction strategies should follow the five stages of protection activity, as depicted in Figure 3.

Figure 3 Five stages of CI protection strategies

Countermeasures

Security planners should select countermeasures keeping in mind the concepts of system security, layered or overlapping security and system integration. They consist of two categories:

- Permanent security measures identify indispensable security investments and relevant means to be employed permanently. This includes information concerning technological measures and organisational measures; control and verification measures; communication; awareness raising and training; security of information systems.

- Temporary (graduated) security measures are in place according to varying risk and threat levels.

Plan maintenance and adaption

Finally, the organisation must ensure that the OSP remains up to date and responsive to the dynamic changes in transportation systems. Ideally, plans are scalable and upgradable on a flexible timeline with sufficient sensitivity to external security factors. The OSP recommends programmatic scheduled plan reviews periodically – at least every six months to a year. The document also provides guidelines on how to conduct this review:

- identify areas to update
- determine completeness
- reassess roles and responsibilities
- review factual information (e.g., names and phone numbers included)
- re-evaluate employee knowledge and awareness (training assessments)
- revise programs and procedures included in the OSP.

The OSP also suggests that the occurrence of certain events requires planners to accelerate the scheduled conduct of a review. Such events include changes of the organisational structure (new general manager), operation (e.g., new bus line), infrastructure (e.g., new bus depot) and changing external relations of an agency (e.g., new supplier).

3.2.5 Implementation plan

This phase depicts the procedures for implementation after the previous steps have been completed and approved by the stakeholders. It consists of three main sections, which take the process from planning through implementation, training and testing to public awareness. Following a successful implementation, ongoing training and monitoring ensures that your site and employees remain focused to all threats.

Physical security

Consistent with effective security planning is the need to deploy appropriate risk reduction methods. This section presents tools and countermeasures that should be considered in the implementation phase for improving the security level.

Physical security countermeasures are distinguished by the layers of security they are part of (DOT – Federal Transit Administration, 2004). These layers vary according to the level of protection they provide for the core assets. Referring to this concept, the impact of countermeasures increases as core assets are approached. The perimeter layer (e.g., fences, lighting) as well as the exterior layer (e.g., visual screening of passengers) are sufficient for the protection against minor threats. Ensuring security in the case of more severe risks, however, requires an interior (well-trained personnel, locks/sensors) and even a restricted layer (e.g., CCTV, biometric access control system).

The actual decision on countermeasures in any given situation depends on its utility. Transportation agencies must examine threats and identify the most useful means to

reduce the connected vulnerabilities to an acceptable level. Utility is not solely a factor of cost. Less expensive and more effective solutions are available which the agency can select to meet security requirements. After that, the agency should return to the concepts of systems approach, layered security and systems integration to decide on how to reduce security vulnerabilities.

Information security

A key element is to protect information systems both in the context of a business service function and, most importantly, systems that control the operations. The initial phase identifies stakeholders within the business interested in ICT assets. The vulnerability assessment localises existing risks and the importance of capturing them in the OSP implementation.

Information systems security does not only refer to firewalls, but also to the prevention of access to the systems themselves. Traditionally, these systems have been closed and therefore are difficult to penetrate. In the course of the integration of business operation platforms, vulnerabilities have been exposed that require more detailed management. Some of the systems described in the physical security are part of this section as well, such as process control, intrusion detection systems, IT network architecture, firewalls and remote access.

Personnel security

An effective personnel RM regime seeks to:

- reduce the risk of employing personnel likely to present a security concern
- minimise the likelihood of employees becoming a security concern
- implement appropriate security measures.

The use of these three steps should ensure an organisation to reduce the risk of information theft, unauthorised disclosure and terrorist acts by insiders, thereby protecting the organisation's assets. Furthermore, an organisation could implement a number of defence methods to avoid such threats:

- Employment pre-screening (vetting): check employment applicants on required preconditions and certain credentials.
- Annual security appraisal questionnaire: short standardised questionnaires to be completed annually by the subject's direct supervisor.
- Ongoing monitoring: regular but infrequent audits of security systems to ensure that the personnel adheres to security policies and procedures of the organisation.

Public awareness

The sharing of valid, timely and reliable information with the media and the public is significantly important for a Transport CI to maintain a high-level sense of security in its facilities, as well as for shaping and maintaining the company's reputation. Essentially, public awareness bases on three axes of communication:

1 Factual information: it creates a trustworthy relationship with the media by sharing reliable and unbiased information.

2 Trustful relationships between the CI operator and the public: this also includes informing the public and raising their awareness.

3 Effective communication responses to and management of critical incidents: this level emphasises the need to establish communication rules for operation during emergency. It should provide immediate and reliable information and contribute to an effective and successful management of the crisis.

Main communication and public awareness tools are:

- press releases
- statements
- public announcements and interviews (including press conferences)
- informal communication with media representatives.

Training

The employees of transportation agencies are a critical resource for maintaining safe and secure operations. However, transportation agencies cannot assume that employees will focus on security issues without training. They need to receive security awareness orientation to prepare them for their security responsibilities. After that, employees must practise the theory to reinforce a security awareness culture in the agency. Establishing a security culture for all employees is mandatory for maximum security in an organisation.

The personnel should be familiar with the OSP. Any staff member holding key positions, as identified in the OSP, should be trained in the assigned duties. Organisational security directors are responsible for this training. Furthermore, the security organisation associated with the facility and any assigned security specialists may provide assistance, such as the preparation of training schedules and materials.

Tests and exercises

Exercises simulate critical situations where decision-making tools are applied and employees are familiarised with the OSP. They are an effective and cost-efficient method of validating the plan, identifying room for improvement and soliciting for feedback.

Exercises may be discussion-based (e.g., seminars, workshops, tabletop), operations-based (e.g., drills, functional, full scale) or any combination of these two. They may be specific for one facility or part of a cooperative exercise program. Exercises should encompass all aspects of the OSP, i.e., also the check of communication and notification procedures, elements of coordination and the availability of resources. An exercise should take place annually with participants of all organisational levels.

4 General discussions

The present research work is based on qualitative information from semi-structured expert interviews and discussions. There was less focus on statistical evidence, but rather

on expert assessments, profound insights and the identification of strategies for a further development of the EPCIP. After establishing trustful communication, interviews have been conducted with many experts in a wide variety of transport regions and the results and conclusions can be considered as valid. However, future work should aim to involve experts from all European transport regions and to repeat the study regularly in order to capture the progress in transport security.

Based on the outcomes of the EUSTO project as depicted in the sections above, EPCIP, and particularly the directive 2008/114/EC, is a good tool for CI operators and stakeholders. Nevertheless, given its non-mandatory and generic nature, they have struggled to be settled in the operators' priority list. Furthermore, lack of knowledge and information (mainly regarding the financial impact of security) among the decision makers of the surface transport CIs gives them the opportunity to ignore or disagree with the necessity of developing security plans, enhancing resilience and complying with the directive.

On the other hand, regulations such as General Data Protection Regulation (GDPR) (European Union, 2016) have pushed all legal entities, including CI, to comply with specific rules regarding the protection of natural persons in terms of personal data processing and free movement of such data.

In addition to the above, efficient tools should be developed and used in order to support the implementation of directives and regulations. Such tools consist of EU-funded projects, e.g., EUSTO or national funded projects, e.g., "Targeted actions for enhancing the protection of national characterized European Critical Infrastructure," which aims to support the implementation of the directive 114 in Greece. The development of security plans models (e.g., OSP model) for CI protection is one target of the project.

5 Conclusions

This paper is a comprehensive approach to support the further development of the EPCIP in the field of surface transport.

Incidents of attacks on public transport have shown emerging threats that stakeholders have to face. Particularly, digital technologies constitute new possible risks that have to be addressed. On a European stage, this is ensured by the EPCIP, particularly the directive 2008/114/EC, which is reviewed in this article.

The assessment of the EPCIP during the EUSTO project (Chapter 2) clearly shows: CI protection is more relevant than ever and the EPCIP provides a useful set of instruments for the protection of CIs. Taking into account that each EU member state has its own legislative framework, necessities and conditions, many experts assess the directive 2008/114/EC as a tremendous step towards increased security. In detail, it has fostered the identification of CIs and the development of security plans and measures. The process has become more explicit and transparent. Member states have analysed their infrastructure and developed individual strategies. Public transport operators have improved their level of information on their criticality status.

Beyond the assessment of the legislator framework, this paper provides a constructive guideline on how to implement an essential part of the EPCIP: the *OSP*. EUSTO built common guidelines for developing OSPs for surface transport CIs that have an EU

dimension, based on industry best practice, in pursue of the objectives of directive 2008/114/EC. The implementation of such an OSP has the following benefits:

- it integrates security into the daily business of the transportation organisation
- it guides personnel towards prevention and effect mitigation of security incidents
- it defines resource and training requirements for staff and equipment
- it ensures a clear division of tasks and responsibilities
- it identifies information requirements for security incidents.

Through two years of research, EUSTO has identified the following challenges and gaps that need to be addressed and further elaborated by the surface transport operators:

- *Extension, transparency and harmonisation of risk assessment methods:* administrations and operators apply different methods for assessing risks, threats, vulnerabilities, impacts and probabilities. They are neither transparent nor harmonised, more detailed guidance is necessary. The focus of the identification method should shift from impact assessment to risk assessment encouraging cross-sectoral considerations.
- *Collaboration and cooperation:* it is obvious that information exchange between CI operators/owners and administrations, especially across borders of organisations and countries, is still unsatisfying. Meeting future challenges is only possible with cooperation and collaboration between the relevant stakeholders in and outside the EU. The EPCIP should focus on this and provide appropriate regulations, incentives and tools for sharing best practices. Awareness, collaboration and cooperation can be triggered by exchange initiatives and platforms (as, e.g., EUSTO, CIWIN) which need orchestration and long-term oriented financing. Interoperable technologies for sharing information should be introduced.
- *Adequate financial resources and fair cost allocation:* stakeholders are reluctant to identify and designate infrastructures as CIs because they fear additional efforts. So far, only large operators can afford to employ security experts. An updated regulation should provide advice on the financial responsibility for security measures. The capabilities of the NCPs should be strengthened.
- *Minimum standards:* the directive already specifies minimum requirements on OSPs that should be extended to cover aspects such as qualification of security staff or coverage with CCTV. Continuous updates of security plans are necessary in the course of changing circumstances.
- *Trainings and exercises:* are extremely important: the directive should provide explicit guidance on that.
- *Public awareness:* is a key that should be increased by effective campaigns.

In order to overcome these gaps and address these challenges, further work should be implemented from different stakeholders, such as surface transport operators, the European Commission, policy makers, technology providers and research institutes. Some identified possibilities for future work are the following:

- Transformation of directive 2008/114/EC into a regulation at an EU or national level.
- Development of specific security models/plans per sector, such as transport, taking into consideration the interconnection and interdependencies with other CIs.
- Enhancement of awareness and information of surface transport CIs on continuously evolving and emerging threats.
- Trainings and exercises at an EU and national level for the surface transport sector, including other sectors (e.g., energy, telecommunication, etc.) that have an indirect impact on their services.

Finally, a general remark: any international harmonisation must also consider varying conditions and necessities, there is not one uniform solution for every operator.

References

AFP (2015) *North Korea Suspected of Hacking Seoul Subway Operator: MP*, Security Week.

Alcaraz, C., Fernandez, G., Roman, R., Balastegui, A. and Lopez, J. (2008) 'Secure management of SCADA networks', *New Trends in Network Management*, Vol. 9, No. 6, pp.22–28, NICS Lab Publications [online] https://www.nics.uma.es/publications (accessed 23 April 2018).

Baker, G. (2008) 'Schoolboy hacks into city's tram system', *Daily Telegraph*, 1 November [online] http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html (accessed 23 October 2017).

BBC (2016) *Brussels Explosions: What we know about Airport and Metro Attacks*, 9 April [online] http://www.bbc.com/news/world-europe-35869985 (accessed 26 April 2018).

Bullock, J.A., Haddow, G.D. and Coppola, D.P. (2017) '7 – transportation safety and security', *Homeland Security*, 2nd ed., pp.169–188, Butterworth-Heinemann.

Cai, N., Wang, J. and Yu, X. (Eds.) (2008) *SCADA System Security: Complexity, History and New Developments*, Institute of Electrical and Electronic Engineers (IEEE), Daejon, South Korea.

CNN Library (2017) *July 7 2005 London Bombings Fast Facts* [online] https://edition.cnn.com/2013/11/06/world/europe/july-7-2005-london-bombings-fast-facts/index.html (accessed 24 April 2018).

Cohen, F., Phillips, C., Painton Swiler, L., Gaylor, T., Leary, P., Rupley, F. and Isler, R. (1998) 'A cause and effect model of attacks on information systems', *Computers & Security*, Vol. 17, No. 3, pp.211–221.

Colarik, A. and Janczewski, L. (2015) *Establishing Cyber Warfare Doctrine*, Palgrave Macmillan, London.

Dolnik, A. and Pate, J. (2002) *2001 WMD Terrorism Chronology*, 18 September [online] https://www.nonproliferation.org/2001-wmd-terrorism-chronology/ (accessed 30 October 2017).

DOT – Federal Transit Administration (2004) *Transit Security Design Considerations Final Report*, Final Report.

European Commission (2004) *Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Critical Infrastructure Protection in the Fight Against Terrorism*, Brussels.

European Commission (2006) *Communication from the Commission on a European Programme for Critical Infrastructure Protection*, 2006th ed., Brussels.

European Commission (2008) *Council Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection*, Brussels.

European Commission (2012) *On the Review of the European Programme for Critical Infrastructure Protection (EPCIP)*, Brussels.

European Commission (2013) *Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection – Making European Critical Infrastructures more Secure*, Brussels.

European Commission (2014) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: on a new EU Approach to the Detection and Mitigation of CBRN-E Risks*, 2014th ed., 5 May, Brussels.

European Commission (2017) *European Commission: Migration and Home Affairs* [online] https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en (accessed 12 May 2017).

European Union (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*, 27 April, Brussels.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. and Laplante, P. (2011) 'Dimensions of cyber-attacks: cultural, social, economic, and political', *IEEE Technology and Society Magazine*, Vol. 30, No. 1, pp.28–38.

Giannopoulos, G. and Schimmer, M. (2011) *Memorandum on the results of the sixth Workshops on the Implementation and Application of the Directive 2008/114/EC*, 1–2 December 2011, European Commission Join Research Centre (JRC), Publications Office of the European Union, Luxemburg

Han, C. and Dongre, R. (2014) 'What motivates cyber-attackers?', *Technology Innovation Management Review*, Vol. 4, No. 10, pp.40–42 [online] http://timreview.ca/article/838 (accessed 23 April 2018).

ISO (2009) ISO 73:2009-11 [online] https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en:sec:3.5.1.3 (accessed 26 April 2018).

Jenkins, B.M., Butterworth, B.R. and Shrum, K.S. (2010) *Terrorist Attacks On Public Bus Transportation: A Preliminary Empirical Analysis*, Mineta Transportation Institute, College of Business, San Jose State University, San Jose.

Lazari, A. (2014) *European Critical Infrastructure Protection*, Springer International Publishing, Switzerland, 2011.

Monterey WMD Terrorism Database, *Monterey Terrorism Research and Education Program* [online] http://wmddb.miis.edu/ (accessed 26 April 2018).

Naeem, W. (2012) 'COLREGs-based collision avoidance strategies for unmanned surface vehicles', *Mechatronics*, Vol. 22, No. 6, pp.660–678.

New York Times (2015) 'French premier warns of risk of chemical attack', *New York Times*, 19 November [online] https://www.nytimes.com/live/paris-attacks-live-updates/french-prime-minister-warns-of-risk-of-chemical-attack/ (accessed 30 October 2017).

Olson, K.B. (1999) 'Aum Shinrikyo: once and future threat?', *Emerging Infectious Diseases*, Vol. 5, No. 4, pp.513–516.

Weiβ, C. (2011) 'V2X communication in Europe – from research projects towards standardization and field testing of vehicle communication technology', *Computer Networks*, Vol. 55, No. 14, pp.3103–3119.