22/06/2020

Version no. 1.0

Security of Explosives pan-European Specialists Network

D6.4
EXERTER 4th report on innovations, standardisation and exploitation within SoE

FOI
KEMEA
FhG-ICT
FhG-EMI
ENEA
BKA
INTA

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no. 786805

D6.4
EXERTER 4th report on innovations, standardisation and exploitation within SoE

Main Report **Main Author(s)**	
Name	*Organisation*
Matilda Ågren	FOI
Ola Norberg	FOI
Johannes Schneider	FhG-EMI
Ioannis Daniilidis	KEMEA
Roberto Chirico	ENEA
Rasmus Schulte-Ladbeck	BKA
Tina Fröhlich	BKA
Christian Ulrich	FhG-ICT
Frank Schnürer	FhG-ICT
Lara Hettmanczyk	FhG-ICT
Juan José Navlet Salvatierra	INTA
Miguel Ángel Ropero Azañón	INTA
Carlos López Pingarron	INTA
Contributors	
Malte von Ramin	FhG-EMI
Pete McCutcheon	PSNI
Chris Nolan	PSNI
Jonathan Middleton	PSNI
Bruno Filipe Bertão Pinto	PSP
Tomislav Vukoja	MUP
Oscar van der Jagt	TNO
Anneli Ehlerding	FOI
Annex 1: Notes on exploitation support (Consortium confidential) **Main Author(s)**	
Name	*Organisation*
Juan José Navlet Salvatierra	INTA
Miguel Ángel Ropero Azañón	INTA
Carlos López Pingarron	INTA
Annex 2: Alternative plot options (EU-Restricted) **Main Author(s)**	
Name	*Organisation*
Ioannis Daniilidis	KEMEA

Annex3: Practitioners’ requirements and capability gaps (EU-Restricted) Main Author(s)	
Name	*Organisation*
Ian Tippet	ICPO
Ola Norberg	FOI
Contributors	
Oscar van der Jagt	TNO
Rasmus Schulte-Ladbeck	BKA
Matilda Ågren	FOI
Patrik Krumlinde	FOI
Workshop participants	

Document information	
Version no.	*Date*
1.0 Final	22/06/2020

Summary

This document is the fourth of the 6-monthly Deliverables on Analysis and Recommendations. It follows the structure described in EXERTER D6.1, where the yearly project cycle, the interaction between the Work Packages, and the role of the Counter Attack Coordinators is outlined in detail.

The aim of the report is to produce tangible and useful output for all Security of Explosives (SoE) stakeholders. The deliverable summarises and analyses the findings on innovations, standardisation and exploitation related to this year's attack scenario: A public transportation scenario based on the Madrid train bombings that took place on March 11, 2004. It also provides the updated user requirements short list and describes potential emerging threats.

Three security classified annexes are connected to this report, Annex 2 (EU-Restricted) and Annex 3 (EU-Restricted). Annex 2 contains alternative plot options that can be considered in the analysis and Annex 3 contains identified requirements and gaps related to this year's scenario identified at the workshop in Freiburg. The last annex, Annex 1, is unclassified and contains project internal notes for the EXERTER consortium regarding the work on exploitation support.

Contents

1 Introduction

1.1 Background

EXERTER connects 21 practitioners from 13 EU Member States (MS) and associated countries across Europe into a Network of Explosives Specialists. The network aims at identifying and promoting innovative methodologies, tools and technologies that will offer solutions in the fight against terrorism and serious crime, i.e. enhancing the overall Security of Explosives. The core of the EXERTER network brings together experts coming from Law Enforcement Agencies (LEA) and Military Institutes, Governmental and Civilian Research Institutes, Academia and Standards Organisations.

The main objectives of EXERTER are:

- Providing solutions to practitioners in the field by extrapolating terrorist threats and attack strategies from recent incidents and matching these with existing and emerging technologies and tools
- Ensuring the practice-relevance of R&D activities by defining end-user requirements and pinpointing existing capability gaps
- Supporting practitioners as well as academia, developers and innovators in their search to find potential industrial partners who have the capability to exploit the innovations into products
- Enhancing practitioner’s operability by supporting standardisation and certification bodies as well as regulators with standardisation and certification priorities in order to facilitate comparison of SoE products and procurement
- Enabling a long-term cooperation among explosives specialists in the security area beyond EXERTER

Though being a self-sustaining network in terms of expertise, the goal of EXERTER is to expand and to reach out to the entire Security of Explosives community to facilitate the interaction among end users, industry and academia and to promote innovation and uptake.

EXERTER has established an End user and Expert Community (EEC) that will be expanded during the course of the project to include relevant stakeholders. The project results will be disseminated through yearly workshops and through interaction activities with stakeholders throughout the course of EXERTER.

1.2 Objectives and scope of the report

This report is the fourth of the 6-monthly Deliverables on analysis and recommendations in the EXERTER project. It aims at summarising and analysing information on requirements, innovations, standardisation and exploitation related to the yearly scenario, and present tangible results for the stakeholders. This year’s scenario is a public transportation scenario based on the Madrid train bombings, March 11, 2004.

The scenario and identified key elements, connected to each counter attack domain, have been described in deliverable D6.3, along with a selection of possible alterations of the scenario. A brief description is also given here in Section 3 and in Annex 3.

The scenario is used as a framework to highlight different aspects of the explosives threat, and for working with these aspects within research and innovation, standardisation and exploitation. Four different counter attack domains, referred to as Prevent, Detect, Mitigate and React (see Figure 1), are continuously pursued and analysed throughout the project. The countermeasures under these four domains differ technically and operationally, and have, to large extent, different sets of users and stakeholders, thus setting a wide scope for the EXERTER network.

Figure 1. The counter attack domains addressed by EXERTER.

This report presents the findings from the different areas in EXERTER related to the second yearly scenario, and its content is made up by internal deliverables and information from the different work packages in EXERTER. The information in this deliverable reflects the work performed in the different parts of the project to date, and it is concluded by preliminary analyses for the different counter attack domains.

1.3 *Outline of the report*

Although the focus for this report is the 2nd year scenario, some work in the project span wider than one scenario. The evolution of threats and attack strategies is one such area. This work is continuously studied in the project, and a report on threats and attack strategies used in past events have now been finalised, which is presented here in Section 2. This information can e.g. be used as a support when the defining the next yearly scenarios in EXERTER.

Section 3 gives an overview of the 2nd yearly scenario, an attack in the public transportation system. More information about the scenario is presented in Annex 3 to this report, as well as in deliverable D6.3. A selection of alternative plot options that can be considered is presented in Annex 2.

Related to the scenario, the practitioners' requirements and gaps, extracted from the workshop in Freiburg, are given in Section 44 and Annex 3. In the following sections, Sections 5 to 7, the status of the work and the findings to date related to the scenario are presented. The information serves as basis for further analyses. Section 5 provides an overview of ongoing and completed research projects, Section 6 summarizes findings on standardisation, certification and regulation, and Section 7 gives a review of products and exploitation efforts.

Section 8 concludes the report with analyses and recommendations related to the scenario.

Three annexes are connected to this report. Annex 1 is a consortium confidential annex that contains forms with interview topics and lists connected to the work in exploitation support. Annex 2 contains alternative plot options that can be considered for an attack, and Annex 3 reports on the gaps and requirements identified at the workshop in Freiburg. Annex 2-3 are security classified.

2 Background to threats and attack strategies

In EXERTER, identifying the evolution of threats and attack strategies is essential in order to assess gaps and requirements, and perform analyses in the context of new threats. It is of fundamental importance that knowledge and analysis of past events will generate understanding and projections of the emerging threats and attack strategies and the evolution of these. The focus for this part of the work is to study these past terrorist attacks, as well as possible attacks occurring during the time of the project, in order to draw conclusions on new trends and patterns of threat and attack strategies, and to extrapolate these into possible predictions of future events. The work supports the scenario definition and is performed in conjunction with all other parts of the project.

This section gives a general overview of treats and attack strategies used in past events, as well as identifies some emerging trends. The information is not specifically connected to this year’s scenario, but rather serves as a background for the continued work in EXERTER.

The fundamental structure is laid through the identification of key elements that define the threats and attack strategies, which lead to three pillars that can describe and determine any scenario; Threat, Vulnerability, and Attack Strategy. Varying the parameters associated with said pillars, future scenarios can be generated or older scenarios be tweaked; such parameters may be technology or procedure oriented.

The project internal report that has been the basis for the information in this section, has also been formulated as a review article, written by the EXERTER partner KEMEA, that will be published in the book series titled Security Informatics and Law Enforcement by Springer. The article sheds light upon the dynamic nature of terrorism over the past decades, concentrating on the threat raised by the use of explosives. It provides an overview of the terrorist threat by adopting a historical and legal perspective, as well as of the past and currently implemented terrorist attack strategies. Based on open sources it presents deduced conclusions on emerging trends and patterns, which could further be the basis of plausible scenarios and predictions of future incidents.

A shortened form of the article is presented in sections 2.2 to 2.4 below.

2.1 Overview

Technology enablers such as computing and telecommunications (from social media to block chains), introduce the additional dimension of digital and cyber to the terrorism. Recent events and the subsequent investigations have indicated that on-line platforms have changed the way individuals radicalise and plan attacks, as well as the speed they mobilise. Individuals, remotely located, coordinate and conspire online, often without having any direct connection or physical interactions with a terrorist organization or fellow adherents. Attacks can be carried out in a simple manner, with a knife or a car.

Furthermore, successful attacks inspire further attacks by like-minded supporters; nowadays, local violence is increasingly connected to a global network. Some emerging threats and their impact are for example:

- The multiple causes of grievance (e.g. MENA (Middle East and North Africa) conflicts, migration crisis, environment) and globally interconnected crises;
- Extensive manipulation of Internet, social media, and encryption software tools to promote and empower radical messages; and
- Differentiated modus operandi by the use of new developed technology, from terrorist networks to lone actors and autonomous terrorist cells.

It is important that we define the threat, otherwise we cannot stop it, and it is crucial that a threat is designated and quantified. Furthermore, and equally important, is that we understand the threat, otherwise we can't defeat it; hence, there is a need for research & training to understand the ideologies that will lead to the key influencers, the justification for violence, and radicalization pathways for those enticed to join terrorist groups.

2.2 Review of terrorist threats

In this section a conceptual definition of terrorism is being approached, in tandem with the delineation of its evolutionary path until the current historical juncture. Subsequently, a series of contemporary developments in modern terrorism are being illustrated, encompassing the so-called Foreign Terrorist Fighters (FTFs) threat as well as the terrorist landscape in the European territory.

2.2.1 Defining terrorism

At EU level, the definition of the term terrorist offences is specified in the Directive 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism. Despite the existence of working definitions, few terms and concepts in modern political discourse present such a plethora of conceptual approaches as in the case of terrorism. The lack of a commonly accepted definition can be attributed to the fact that terrorism is a highly subjective term, with a strong political tone, depending on the subject's experiences and personal views.

2.2.2 Origins and typologies of terrorism

Modern terrorism is considered to have originated with the French Revolution, when the term "terror" was first coined (1795) to refer to a policy systemically used to protect the fledgling French republic government against counterrevolutionaries.

From the French revolution, through David Rapoport's theoretical scheme of the "terrorist waves" constitutes an endeavour to shed light on the evolution of modern terrorism. According to the American academic, since the end of the 19th century there have been four "terrorist waves", which he describes as "Anarchist", "Anti-colonial", "New Left", and "Religious" (Rapoport, 2002).

Anarchism comprises the first of Rapoport's waves. Between 1880-1905, anarchist terrorists assassinated the Austrian empress, the king of Italy, French and American Presidents, as well as dozens of citizens, accused as being part of the bourgeoisie. Although the pursued international revolution did not materialise, anarchists exerted a significant influence, most notably through the so-called "propaganda-by-the-deed" in which acts of individual heroism sought to elicit similar chains of reaction (Neumann, 2016).

The Anti-colonial wave emerged in 1930 and reached its peak in 1950. The violent groups, that composed it, were integrated in the population and aimed at combating foreign domination, leading to the eventual withdrawal of colonial forces. This wave laid the foundations for the conversion of terrorism in the late 1960s from a mainly local phenomenon to a global security issue (Hoffman, 2006).

The New Left was largely composed of members of the upper middle class. Its central aim was the emergence of a new, socially just and anti-authoritarian society situated on socialist principles, but in a distance from the ongoing version of socialism in the Eastern coalition countries (Neumann, 2016). The basic strategy was to incite the socio-political overthrow from the urban areas by waging spectacular attacks against governmental targets and "systemic agents".

The onset of the Religious wave dates back to 1979, a year marked by the Iranian revolution, the USSR invasion of Afghanistan, and the capture of the great mosque in Mecca by Sunni Muslims whilst, according to the Muslim calendar, 1979 was the beginning of a new century (Neumann, 2016). Murders and hostages comprised common practices of the new Left wave, but "suicide attacks" were the most impressive and innovative tactics, with Islamist terrorists being internationally networked. During this Religious wave, a terrorist organization appeared, with apparently "pioneering" methods of recruiting and operating in the history of terrorism, – al-Qaeda.

2.2.3 Key developments in modern terrorism

The contemporary elements that compose the nature of terrorist activity are briefly addressed through the exploration of the notion of "new terrorism", the depiction of the concerns associated with the FTFs threat, along with the overall impact of terrorism at European level during the past five decades. The sometimes-broad use of the term "new terrorism" (Simon, 2000), was adopted during the period of the terrorist attacks of 11 September 2001 (the heyday of al-Qaeda terrorist organisation) and it bears a number of partially distinct characteristics, summarised in Table 1. New terrorism can also be approached as conducting asymmetric/non-conventional war operations between terrorist organisations and nation-states.

Table 1. Fundamental elements of New and Old Terrorism

	New Terrorism	**Old Terrorism**
Aims	Religiously-inspired, absence of ideological rigour	Predefined set of political, social and/or economic objectives
Methods	Mass civilian attacks; excessive violence	"Legitimate" targets; rules of engagement
Targets	Civilians, infrastructure, officials; soft and -less frequently- hard targets	Symbolic targets (e.g. embassies, banks) or persons representing authoritarianism; hard targets
Structure	Global network and agenda	Hierarchical structure

Since the Syrian conflict began in 2011, thousands of EU nationals have travelled or attempted to travel in conflict zones in Iraq and Syria to join insurgent terrorist groups, such as ISIS/Daesh. This influx of the so-called "Foreign Terrorist Fighters[1]" (FTFs) to Syria and Iraq seemed to have reached, in 2018, a number of more than 40,000 individuals originating from around 110 countries, of which it has been estimated that around 30 % have already returned to their place of origin (European Parliament, 2018).

Currently, the issue of the FTFs remains high on the political agenda at both Member State and EU level inasmuch as it touches upon a broad spectrum of policies, related to the prevention of radicalisation, information exchange at EU level, criminal justice responses to returnees, as well as disengagement/de-radicalisation inside and outside prisons (European Parliament, 2018).

Regarding the terrorist landscape in Europe, the 9/11 attacks have been a key point in redefining the role of terrorism and helping to raise awareness in terms of international security issues. In fact, the global terror attacks have led to an intensive effort to exercise internal control and vigilance in the fight against terrorism. At the same time, new forms of "cross-border coalitions" were established between countries,

[1] According to the UN Security Council and its Resolution 2178, Foreign Terrorist Fighters (FTFs) are defined as "…. nationals who travel or attempt to travel to a State other than their States of residence or nationality, and other individuals who travel or attempt to travel from their territories to a State other than their States of residence or nationality, for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts, or the providing or receiving of terrorist training, including in connection with armed conflict".

with an emphasis on the use of military and civilian power and the overriding aim of ensuring world peace and security (Das, 2016).

Focusing on the last decades of terrorist activities, the attacks of September 11, 2001 signalled the shift toward religiously-inspired terrorism and jihadism. Since then, Europe has witnessed large-scale attacks, such as in Madrid on March 11, 2004, and in London on July 7, 2005. From 2014 onwards, Daesh joined al-Qaeda as a new salafist-jihadist terrorist group, and between 2014 and 2016, Europe was the place of several major terrorist attacks[2].

Nevertheless, alongside the salafist-jihadist terrorist threat, Europe faces a significant rise of the extreme right-wing ideology and extremist action. In particular, extreme right-wing attacks fluctuated from 9 in 2013 to 21 in 2016 and 30 in 2017, namely the highest number of right-wing attacks in Europe since 1994 (Jones, 2018).

2.3 Review of terrorist attack strategies

The inherently fluid nature of terrorism contributes substantially to the upgrade of several terrorist organisations into "lifelong learning entities" (Ganor, 2015). In order to ensure the survival of the organisation, this "learning process" requires the gradual alteration of key elements and tactics of action. The formulation and effectiveness of the latter are crucially underpinned by technological innovations, along with the ability to manipulate democratic institutions and values.

Hence, attack strategies are continually evolving. Prominent elements seen in modern terrorism are the networking structure, driven by technological advances, along with lone actors' individualised terror activities.

An important parameter for modern terrorist organisations is their involvement in the digital world. Indeed, since the early period of al-Qaeda, its online presence was seen as a significant mechanism for the transition to an era of terrorism, characterised by the active role of digital extremist communities with a high degree of resilience. New media and their multiple applications have also facilitated the transformation of pyramidal organisational structures into horizontal networks, in which numerous members are linked by advanced means of communication (Tucker, 2001), (Mockaitis, 2007).

The structural transformation of modern terrorism is the emergence of a variety of operational actors. Amongst them, the salient role of the "lone wolves[3]" can be identified, along with their implemented strategy – the so-called "leaderless resistance". A lone wolf is usually driven by political and/or religious motives, and is commonly without any direct link to a terrorist organisation (training, funding, etc.). Leaderless resistance could be seen as a "confrontational strategy" that encourages involvement in acts of political violence, which are independent of any hierarchical structure or support network (Joosse, 2007). In this way, individuals or small cells can fight against an established power through independent acts of violence, without being centrally coordinated and with limited or non-existent communication between them.

The terrorists' strategy is in many instances driven by rational choices, and preceded by "cost-benefit" analyses, in order to select the most beneficial course of action by effectively offsetting the risk and the costs inherently involved, while achieving its goal and objectives. As such, although in many cases jihadist terrorists are portrayed by the media as maniacs and mentally disturbed killers, they are in fact

[2] E.g. the January 2015 attack against the satirical newspaper Charlie Hebdo, the November 2015 massacre in the Bataclan theater, the 2016 attacks at the Brussels Airport and Maalbeek metro station in Belgium, and the 2016 Nice vehicle attack, as well as the similar attack on a Christmas market in Berlin the same year.

[3] An autonomous perpetrator, who aims to have an impact on the wider community, acting without direct support during the planning, preparation and execution phase of the attack, and whose decision to act is based on inspiration rather than direct guidance from peers (Ellis, 2016).

"disturbingly normal" persons, as they make careful calculations before committing heinous crimes (Hoffman, 2006).

Explosives as the weapon of choice has been a common denominator for many attacks in the EU. The explosives-related jihadist plots, usually aimed at soft targets and mass gathering locations, have commonly used IEDs based on the homemade explosive TATP (Triacetone Triperoxide). In contrast, targets chosen by anarchist extremist groups are mostly state, financial, military, or law enforcement targets, with the anarchist groups utilising simple improvised incendiary devices (IIDs) filled with flammable liquids or IEDs filled with easily accessible explosives materials, such as pyrotechnic mixtures (Europol, 2019a). Commercial explosives have also been used (e.g. Madrid 2004) but they can be difficult for terrorists to acquire, while military explosives are even harder to access, even if explosive remnants of war and illicit trafficking in explosives are still presenting a significant threat to the EU (Europol, 2016).

2.4 Emerging threats and attack strategies in terrorism

This section provides a synopsis of threats and attack strategies, that have already started to manifest themselves in the EU internal security environment, eventually concentrating on the (mis)use of explosives and technology.

2.4.1 General Trends and Patterns in Modern Security Environment

Preventing radicalisation is a significant challenge. A spread of extremist ideologies that further leads to an increased polarisation in society remains of deep concern among EU Member States, including violent Islamist, right-wing and left-wing ideology, as well as how they fuel each other.

Daesh has contributed as a major motivator and inspiration for recent salafi-jihadist terrorism in the EU. The Daesh military defeat in Syria/Iraq have had a significant negative impact on the group's digital capabilities, but it has still maintained its online presence thanks to unofficial supporter networks and media outlets (Europol, 2019a). Although the group currently lacks capacity to coordinate and conduct external attacks, it maintains the intent to perform such operations, potentially using "sleeper cells[4]" (Burton and Stewart, 2008). The returning FTFs have also been highlighted as potential threats, taking into consideration the possibilities of recruiting individuals and thus contributing to the formation of a radicalised European network.

It has been noted that radicalisation in prison remains a considerable challenge, given the potential security risks posed by those convicted of terrorist offences and/or those radicalised in prison that are released.

Regarding strategy, a large number of recent terrorist attacks have been carried out through the use of improvised weapons, like knives and vehicles. These attacks do not require special prior training or extensive logistical support, and the lack of sophistication can make the attacks hard to detect let alone to predict.

Other trends are the use of the so-called "hawala" informal banking system, along with the misuse of credit systems, non-profit organisations, and small-scale business ventures which constitute means of fundraising and financing of terrorism.

2.4.2 The Explosives Threat

In Europe, the unlawful use of explosives is highly related not only to groups or lone actors linked to jihadist terrorism, but also to many organisations and individuals with radical right-wing and left-wing ideologies. In particular, a number of current and emerging trends, with regard to the use of explosives

[4] A sleeper cell is consisted of operatives, who infiltrate the targeted society or organisation and remain dormant until their activation, usually after a prearranged signal or a certain chain of events (Burton and Stewart, 2008).

for terrorist purposes, have been observed (Europol, 2019a). Regarding the IED, there is a shift towards using a broader range of homemade explosives (HME), such as black powder, chlorate mixtures, fertiliser-based mixtures and pyrotechnic mixtures (mainly fireworks). There have also been identified attempts (in 2018) to use IEDs in combination with chemical or biological toxins, something that was promoted in jihadist propaganda and IED-making manuals. In terms of HME and IED production, the trend is that knowledge transfer is enhanced through the use of online, and often encrypted, social networks and forums, and from readily available online open sources (e.g. pyro/explosives enthusiast sites and forums). (Europol, 2019a)

2.4.3 Misuse of Technological Advances

New modi operandi and criminal activities may be enabled by advanced technologies like online trade in illicit goods, virtual currencies, alternative banking platforms, and encrypted communication technologies (Europol, 2019b). For example, the decentralised Darknet markets and cryptocurrencies, that comprise key facilitators for trade in illicit goods, can enable vendors and customers to carry out transactions with high degree of anonymity (Europol, 2019b). Another technological advance that raises important concerns is Artificial Intelligence, and how it can transform the security landscape by becoming a tool for conducting cyber-attacks, target selection, production and spreading of false information (fake news, deep fakes, etc.), as well as for handling AI drones and self-driving vehicles. (Europol, 2019b)

3 Scenario in brief

The second EXERTER scenario, used as basis for the work, workshops and discussions in EXERTER, considers an attack on public transportation with IEDs containing civil explosives. The scenario is based on the 2004 Madrid train bombings. In order to not solely focus work and discussions to a single past event, alternative scenario plots are also considered, including possible emerging threat scenarios.

The 2004 Madrid train-bombing scenario is described in Section **Error! Reference source not found.** below, and a more generic scenario definition is given in Section **Error! Reference source not found.** along with some scenario highlights.

The scenario was presented at the practitioners' workshop in Freiburg November, 19-20, 2019. The participants were then asked to not limit the discussions to only cover the Madrid bombing scenario but to also think of possible future attack scenarios. These alternative and future attack options are collected in Annex 2 to this report. The requirements and gaps collected during the workshop are given in Section 4, and in Annex 3.

3.1 Scenario description

International and national terrorism have had a significant impact on many EU member states in the past decades. However, 2004 Madrid attacks galvanized EU responses and policies to counter-terrorism. These attacks showed that EU was not immune to broad-scale terrorist attacks, prompting EU agencies and governments to work together to prevent future incidents. The Madrid bombings of March 11, 2004 were considered as the "EU September 11."

On the morning of March 11 2004, 10 bombs packed with nails and dynamite exploded on trains heading towards central Madrid. The blasts killed 191 people and injured approximately 1,800. The ten IEDs exploded in four different trains, three additional IEDs were found and neutralized by controlled detonation, and one IED was defused. The bombs were contained in small bags.

The bombings were carried out by a group of young men, mostly from northern Africa, who were, according to prosecutors, inspired by a tract on an al-Qaida-affiliated website that called for attacks on Spain. The aim of the attack is believed to be to kill a large number of people to, in turn, provoke a reaction a few days before the Spanish general elections. The attack is described in the threat, vulnerabilities and attack strategy framework below in **Error! Reference source not found.**. Analysing the attack, it is important to raise the question of the projection of this (or any other past) scenario to the current time with the enablers available; how would a similar scenario develop today?

Table 2. The Madrid train bombings scenario

Threat profile	27 members of a terrorist network, involved in preparation & execution
	Some of them attended Madrid's Islamic worship sites (mosques)
	Inspired by radical websites and online propaganda material
	Suspicious travel patterns and individuals linked to international terrorist groups, like al-Qaeda and the Moroccan Islamic Combatant Group (GICM)
	A few terrorists adopted a violent conception of Islam while in prison facilities of Spain, where some of them co-existed with members of organised crime groups
	Hence, nucleation of threats in a religious frame / environment
	Acquisition of explosives (dynamite) through Spanish criminal groups

Modus Operandi	A property in the city of Chinchon was rented to become their operational centre
	Usage of prepaid cell phone cards, obtained by showing fake identities
	13 or 14 bombs were placed on 4 different trains at Alcala de Henares station
	Between 07:39-07:49, 10 of the bombs detonated in 4 locations.
Vulner-abilities	Radicalisation at religious sites and “prison nexus” between terrorists and criminals
	Erroneous claims of evidence, purportedly indicating the terrorist organisation ETA
	Inadequate international and EU law enforcement cooperation (intelligence sharing)
	Lack of professional structures that could receive and analyse information, thus assessing existing/emerging risks
	The fight against global terrorism had not received due priority and preventive response at EU level
Attack strategy	Spain supports US in Iraq. People’s Party in favour of Spanish intervention, and Socialist Worker’s Party wants to withdraw
	Al-Qaida warns Spain to leave or face retaliation
	Oncoming parliamentary elections

3.2 Generalised scenario context and highlighted scenario aspects

To not limit discussion to an historic event, the yearly scenario, a public transportation scenario, is considered as a generalised event based on the Madrid bombings.

The generalised scenario is a coordinated attack on the public transportation system in a city. The time for the attack, (morning with many commuters) is chosen to maximise the number of victims. The perpetrators are organised in one or more cooperating terrorist cells.

For the IEDs, commercial explosives and detonators, triggered by mobile phone alarm functions, are used. The explosives and detonators are acquired via criminals. The IEDs are equipped with metal objects aimed to function as shrapnel to maximise the effect. Certain highlighted aspects of the attack are listed (see **Error! Reference source not found.**) in respect to the different phases in the terrorist timeline.

Table 3. Key elements for the second yearly scenario, a public transportation scenario based on the Madrid train bombings that took place on March 11, 2004.

Prevent	Access to commercial explosives including detonators
	IEDs assembled in urban environment
Detect	Commuter trains, public area, no security checkpoints
	Simultaneous detonation, programmed
	IEDs concealed in rucksacks and bags
	Commercial explosives + shrapnel
Mitigate	Target is crowded and publicly accessible
	Train: Closed or nearly closed (small) confinement
React	Emergency services arrive at scene
	Collapse of phone network

	Prioritisation of resources at the scene
	Collection of evidence

3.3 *Alternative plot options to consider*

In relation to this year's scenario, a selection of alternative plot options that can be considered in order to encompass a wider base for discussions, analysis and recommendations. Some elements that could be considered for an alternative plot are listed in Annex 2.

4 Identified requirements and gaps

The identified requirements and gaps are provided in an EU Restricted annex, Annex 3, to this report. It contains the input received from stakeholders concerning requirements and gaps connected to security of explosives capabilities.

Practitioners' ideas and knowledge on requirements and gaps will support the continued work in EXERTER. Information regarding requirements and gaps is based on responses to questions posed in a Table-Top Exercise run during the EXERTER workshop in Freiburg, November 2019. A preliminary shortlist with these requirements was included in deliverable D6.3. An updated version is now provided in Annex 3.

The workshop was conducted by dividing the participants into four teams, 5-6 participants in each team, previously selected by the workshop facilitators to encourage an even distribution of specific skills and experiences. Each team had a leader to facilitate and encourage discussion. The discussions were regularly fuelled by "injects", e.g. new aspects to the scenario to consider. After each inject the teams were directed to provide written responses under the headings 'Prevent, Detect, Mitigate and React'. The teams were assigned time to document their points and time was allocated for the groups to present their findings to the other teams, followed by a question and answer session.

Each team was encouraged to discuss their own ideas and those provided by other teams. They were tasked with considering the best methods for resolving the issues presented under the 'Prevent, Detect, Mitigate, and React' headings. The project's intentions were not to force the exposure of specific operational gaps, but to encourage freethinking, and to support a well-considered and appropriate resolution or innovative response to potential issues.

In other words, participants would be less likely to talk without restriction if they were required to identify weaknesses and capability gaps in their own country or areas of expertise, and therefore the discussions were held around current procedures and capabilities in general.

5 Research review

5.1 *Introduction*

In EXERTER, information about SoE research and innovation projects are continuously collected to create an overview of current and completed research activities. The work involves collection and identification of already finished and ongoing national, European and international Security of Explosives (SoE) research projects, which can help in the fight against terrorist plots.

More than 220 projects have currently been listed. This list includes project names, project descriptions as well as some identified important key elements. It contains only unclassified information about the projects, and will be extended and updated continually. Through communication and interaction with other projects as well as web searches and special workshops or conferences, additional research activities will be identified and included in the research activity list. EXERTER have recently been granted access to a database created by the H2020 project ENTRAP, and the information therein is currently being reviewed.

For every yearly EXERTER scenario, relevant research projects are reviewed with the aim of finding solutions for practitioners' needs and gaps. The relevance of collected information is evaluated with respect to the selected scenarios and to each counter attack domain of the terrorist attack.

5.2 *Review of research activities in the different counter attack domains*

A first selection of the most auspicious research activities, based on the overview of SoE research activities, are presented below for each of the counter attack domains; Prevent, Detect, Mitigate and React. These projects have performed research that potentially addresses some aspect of the practitioners' needs and gaps in the field of SoE relating to this year's scenario (see Section 3). The current list reflects a first selection. It is still tentative, and the presented projects will be further studied in detail to make an updated selection.

5.2.1 Prevent

The year 2 scenario concerns civil explosives in the public transport system. Since the majority of research projects within the PREVENT domain are focused on Home Made Explosives, the selection of research projects has been a difficult task.

Legislation and control are the most important tools for countering the misuse of commercial explosives. However, the aspect that could be addressed in the scenario is the bomb production in a bomb factory, and the release of traces to the surrounding environment in terms of markers or the explosive itself. With this in mind, the preselection of research projects for the 2nd year scenario are projects that were focused on detecting a bomb factory. Note that all of these projects were focussed on Homemade Explosives (HME) rather than civil explosives.

BONAS (EU FP7: BOmb factory detection by Networks of Advanced Sensors): The aim of BONAS was to design, develop and test a novel wireless sensors network for increasing citizen protection against terrorist attacks, in particular against the threat posed by improvised explosive devices (IEDs) devices.

EMPHASIS (EU FP7: Explosive Material Production (Hidden) Agile Search and Intelligence System): The aim of EMPHASIS was to develop a system for detecting ongoing illicit production of explosives and IEDs.

LOTUS (EU FP7: LOcalisation of Threat substances in Urban Society): LOTUS aimed to create a demonstrator system by which illicit production of explosives and drugs can be detected during the preparation and production phase of a terrorist plot.

5.2.2 Detect

For the scenario of the 2nd year following projects were preselected:

DEXTER (NATO-SPS: Detection of EXplosives and firearms for counter TERrorism): This project aims to develop a system to detect explosives and firearms in public spaces, remotely and in real time, without disrupting the flow of passengers. DEXTER consists of three project parts EXTRAS, INSTEAD and MIC. All three are ongoing projects.

STANDEX (NATO-SPS: STANd-off Detection of EXplosives): This project dealt with the stand-off Detection of Explosives on suicide bombers in mass transport. This project, which was supported by the NATO Science for Peace and Security Programme, developed technologies to detect explosives concealed on a person moving through a crowd, for example in a metro station at rush hour.

PREVENT (EU H2020: PRocurEments of innoVativE, advaNced systems to support security in public Transport): PREVENT focuses on pre-empting attacks in public transport by enabling earlier detection of terrorists and potentially dangerous objects, tracking of detected individuals or situations and coordinating the response of security forces. The project is ongoing and undertakes a gap analysis between available solutions, existing standards, on-going research and identified needs, from which it elaborates a multi-dimensional roadmap of innovations and solutions.

CONSORTIS (EU FP7: CONcealed objects Stand-Off Real-Time Imaging for Security, FP7-SECURITY): The project aimed to develop a demonstrator for stand-off real-time concealed object detection, based on millimetre-wave imaging technology, for future implementations of high throughput security screening for European mass markets and infrastructure security.

SUBITO (EU FP7: Surveillance of Unattended Baggage and the Identification and Tracking of the Owner, FP7-SECURITY): SUBITO has researched and developed automated detection of abandoned luggage, fast identification of the individual responsible and the tracking of their subsequent path.

ADABTS (EU FP7: Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces FP7-SECURITY): ADABTS aimed to address one of the key problems, the definition of abnormal behaviour, by extracting characterizations in realistic security settings based on expert classifications and the analysis of CCTV operator behaviour.

Another important EU research activity for the DETECT phase in the context of the 2nd scenario is the ERNCIP Thematic Group (TG) “Video Surveillance for Security of Critical Infrastructure”. This group aimed to identify the activities on video surveillance technologies within the security sector that will assist operators of critical infrastructure in improving their security.

5.2.3 Mitigate

For the scenario of the 2nd year, aligned to the Madrid Bombing 2004, the focus of the relevant mitigation measures is on neutralisation techniques and organisational/management measures that could reduce the number of injuries. There are almost no relevant explosion effects mitigation measures that could be relevant for internal explosions in commuter trains. The following projects were preselected:

SensSE4Metro (National, Germany: Sensor based security and emergency management system for underground metro systems during disaster events): The overall objective of the research within SenSE4Metro is to improve the security of persons in urban underground trains and underground stations in emergencies and catastrophes, resulting from terrorist attacks on underground trains, train stations and natural disasters, such as earthquakes and flooding.

SinoVE Management (National, Germany: Security in open transport systems and railway management): Collaborative research project 'Security in open transport systems and railway management'. Contribution of GFaI: Fundamental investigation of methods for the modelling of risk scenarios in complex transportation infrastructures. Development of an innovative safety management system for transport systems and railway management. Particular focus is placed on transport hubs for passenger transport. By simulating hazard situations, the new methods technically support security forces facing critical situations.

SECURESTATION (EU FP7: Passenger station and terminal design for safety, security and resilience to terrorist attack): The aim of the SECURESTATION project was to improve passenger station and terminal resilience to terrorist attacks and safety incidents through technologies and methodologies enabling design to reduce the impact of blast, fire and the dispersion of toxic agents on passengers, staff and infrastructure.

SECURESTATION considered threats from terrorist attacks and safety incidents caused by blast, fire and accidental or deliberate particle dispersion. The four project objectives were:

1. "To increase resilience of passenger stations and terminals through structural design, interior design, and building services design, realising everyday benefits while designing for security."
2. "To ensure cost-effectiveness of countermeasures through application of risk analysis methodologies to prioritise actions taken in design and operation of passenger stations and terminals."
3. "To deliver a constructive design handbook addressing new build and retro-fit cases to serve as a powerful decision support tool for owners and operators to increase station security and safety from terrorist bomb blast, CBRN attacks involving particle dispersion, and fire events."
4. "To create harmonisation and the standardisation of risk assessment methodologies, technologies and design solutions thereby supporting wide application by the numerous European public transport organisations and associated key stakeholders."

The main focus for SECURESTATION was to produce the necessary tools to build safer and more secure infrastructure whilst providing maximum operating resilience. It covered the development of a risk assessment methodology (including simulation results), specifically focusing on passenger stations/-terminals (a scenario specific methodology) and the development of a constructive design handbook.

SECUREMETRO (EU FP7: Inherently secure blast resistant and fire safe metro vehicles): Increased safety and security of metro vehicles from terrorist attacks by explosives and firebombs through materials choices and design, thereby increasing resilience and reducing the impact of attacks on passengers, staff, infrastructure and property.

The SECUREMETRO project considered threats from conventional explosives and firebombs. The four project objectives were:

1. "To increase metro vehicle resilience to terrorist bomb blast through selection of vehicle materials and structural design. This will reduce injuries from fragments of vehicle materials and improve structural integrity in blast situations, offering greater security to passengers and staff. This includes enhancing the ability of a vehicle to remain on the track and keep moving so that underground rescue is not required. Contribution to structural integrity standard EN12663 will allow wide and interoperable implementation of vehicles offering security by design."
2. "To increase security against a firebomb attack through design of fire barriers and fire suppression technology while also contributing to passenger safety from accidental or vandalism fires. Design of features to prevent the spread of fire and fumes will contribute to standards compliance (prEN 45545 and TS 45545) for fire protection of railway vehicles."
3. "Through increasing resilience of vehicles to blast and fire attacks and reduced damage to adjacent vehicles and infrastructure, speed up recovery following attack, allowing the rail system to "bounce-back" to normal operation quickly."

4. “Reduce the attractiveness of metro systems as a target for attack by reducing deaths and injuries, increased resilience, reducing economic impact and making recovery faster. This will be achieved through wide dissemination of the findings of SECUREMETRO, and promotion of transfer to high speed rail of the vehicle design and technology developed for metro systems.”

5.2.4 React

For the counter attack domain React the following projects have been selected:

HYPERION (EU FP7: Hyperspectral imaging IED and explosives reconnaissance System): The aim of HYPERION was to develop and test a quickly deployable bomb analysis system for on-site forensic analysis after an explosion. Tools and procedures for the stand-off detection and identification of unexploded IEDs were included. This project was intended to develop stand-off detection systems while it was successful in that it developed a capacity to identify visible substances up to 50 m away it was not that successful with regard to mobility. The resulting devices had to be transported on a car to function at the site. The project could fill the gap to detect second devices and visible leftovers of HMEs at the expense of mobility and start-up time of the device.

CHEQUERS (EU H2020: Compact High pErformance QUantum cascadE laseR Sensors): The CHEQUERS Project was intended to develop a man portable explosive identification system with stand-off capability. Where the HYPERION System had a stand-off range of 50 m the CHEQUERS System had a range of only 1-2 m but was easily portable by one person. The aim and potential of the project would be to rapidly deploy a system to identify left-over devices at the attack site but also to help the specialist to secure a bomb factory more easily by identifying potential hazardous substances. The first would be applicable especially with a Madrid type scenario whereas the later use would be helpful in scenarios both like the Madrid bomb lab and like the preparation site of Breivik (Oslo bombing).

SUBITO (EU FP7: Surveillance of Unattended Baggage and the Identification and Tracking of the Owner, FP7-SECURITY): SUBITO has researched and developed automated detection of abandoned luggage, fast identification of the individual responsible and the tracking of their subsequent path. In the Madrid scenario, there were a lot of left over luggage at the sites of the attacks. These unidentified bags, rucksack etc. were all potentially secondary devices or devices that did not function. To identify the responsible individual and automate this process would be a great help for the first responders to achieve security at the sites much faster than in the Madrid case. SUBITO is also interesting for the DETECT phase.

XClanLab (ISFP): The XClanLab project intends to develop an App which could be used by non-specialist end users to identify bomb factories or sites where HME was produced. This could be helpful in the aftermath of an attack to support the uniformed police in finding the site of the bomb preparation as well as identifying supporters of the attack.

SUSQRA (National, Germany: Schutz vor Unkonventionellen Sprengvorrichtungen – Charakterisierung und Quantitative Risiko Analyse, English transl.: Protection against IEDs – characterization and quantitative risk analysis): The aim of SUSQRA is to develop a software which can determine the extent of damage inflicted by IEDs, also for the forensic post blast evaluation. If successful, this project will be useful in the evaluation of an attack and the subsequent improvement of potential security measures in regard to the protection of infrastructure by means of ballistic protection of buildings or modifying transport hubs to minimize damage potential.

6 Standardisation and certification priorities

6.1 Introduction

Work related to standardisation and certification in relation to the yearly scenario and its key elements is presented below. This chapter aims to provide a broad foundation with information that could be of relevance for the continued work with, and analysis of, the 2nd yearly scenario.

Through interactions with practitioners, private sector and standardization bodies relevant for the EXERTER project, a number of relevant standards have been listed (full shortlist available in EXERTER D6.2). From this list, a selection considered relevant in the context of the yearly scenario is presented in Section 6.3. In addition, guidelines, regulations and similar that have been noted by EXERTER partners as interesting or relevant are mentioned in this chapter.

It has been noted, both by (Poustourli & Kourti, 2014) and by EXERTER partners, that many regulations, standards and guidelines in the security area exist on a national level in EU member states, and there are few EU common standards. (Poustourli & Kourti, 2014), representing ERNCIP, also expresses that “Divergent national standards seem to pose a major obstacle for the creation of a true internal market for security, thus hindering the competitiveness of EU industry”.

Regarding the security and safety of public transportation and public spaces, a number of documents and guidelines have been published by e.g. different UK governmental agencies. These guides cover, but are not limited to, the threat from terrorism, and could partly be relevant for all counter attack domains.

For example, the UK Department of transport have published guidelines for security for busses and coaches (DoT, 2018), light rail (DoT, 2014), and stations (DoT, 2012), and Centre for the Protection of National Infrastructure also considers the terrorism threat in the published guide *Protecting against terrorism* (CPNI, 2017). This publication offers advice for any organisation looking to protect against the risk of a terrorist act or limit the damage such an incident could cause. Other guides, such as *Crowded Places Guidance* (NaCTSO, 2017), is published by the National Counter Terrorism Security Office. This guide covers several categories of public spaces, among them transport. On the webpage of Secured by Design - Official Police Security Initiative, several guides for counter terrorism can also be found. One example is the *Resilient Design Tool for Counter Terrorism* (SBD, 2020), which is a guideline to help key decision makers to consider the proportionate use of counter terrorism design features in developments planned for crowded public places.

The International Union of Railways has also published security guidelines. For example regarding preventive measures against terrorist acts on railway premises (UIC, 2013), about station security for station business (UIC, 2017), and for managing suspicious items in railway premises (UIC, 2019a), (UIC, 2019b).

6.2 Issues

Some issues that have been raised by people in the network in connection with standardisation, certification and regulations are that:

- There are laws/regulations that might hinder the work/progress in the field of SoE. The regulations and thus the effects, vary between countries. One example is the regulations regarding who is allowed to handle explosives, which may be an obstacle for e.g. universities to perform research that could lead to the development of new detection systems etc. The problem is however perceived to be smaller for developing software and IT-technology.

- Limited funding possibilities, and how this is regulated in each country, is a hinder. If some law/regulation is passed, e.g. new stronger measurements in border control, it is noted that this area then might need extra funding (equipment, software, human resource). Controlling all regulations also requires resources, both monetary and personnel.

6.3 Overview of standardisation and certification initiatives

Technical Committees (TC) and standardisation initiatives with relevance for EXERTER have been assessed, and a selection of them is listed below for the respective counter-attack domains.

Standardisation entities of particular interest are for example CEN/TC 391 Societal and Citizen Security and ISO/TC 292 Security and resilience.

6.3.1 Prevent

6.3.1.1 Standardisation initiatives

A subset of the standardisation initiatives that have been identified as relevant for the prevent domain in the context of the yearly scenario are listed in Table 4.

Table 4. Standardisation entities relevant for the counter-attack domain Prevent

Entity	TC/WG	Name	Description
CEN	TC 321	Explosives for civil uses	Standardization of explosives substances and articles, including safety requirements, terminology, categorization and test methods. Pyrotechnic articles and ammunition are excluded and explosives intended for use by the armed forces or the police are also excluded.
CEN	TC 325	Crime prevention through building, facility and area design	Development of European standards for the prevention of crime at industrial facilities, educational institutions, hospitals, residential building areas, department stores, squares and public meeting places through building, facility and area design. The standards will include their area of application, the corresponding strategy, security levels, building and area layout, application of construction elements, roads and pavements. The standards may be applied to new and significantly refurbished buildings, facilities and areas. The standards will not deal with building products and security systems components.
CEN	TC 391	Societal and Citizen Security	The main objective of CEN/TC 391 is to elaborate a family of European standards, standard-like documents (e.g. procedures, guidelines, best practices, minimal codes of practice and similar recommendations) in the Societal and Citizen Security sector including aspects of prevention, response, mitigation, continuity and recovery before, during and after a destabilising or disruptive event. Verification and training will also be considered. CEN/TC 391 will not deal with issues already dealt in other TCs. Concerning technology, CEN/TC 391 may identify needs in product standardisation, but this will not lead to direct action by this CEN/TC. These issues shall be communicated to those CEN, ISO or other TCs working within the framework of these specific products. Where other TCs do not address the identified areas, then CEN/TC 391 will develop the standard(s) or proposed deliverables where appropriate. The standardisation activities will consider the following main issues related to Societal and Citizen Security: - Products and services (equipment, communication, information, goods, transport, energy,

			cultural inheritance and properties); - Infrastructures (roads, ports, airports, rail stations, bridges, factories...); - Stakeholder needs and requirements, potential conflicts; - Relationship (cultural and geographical diversity); - Citizen requirements and vulnerabilities, including privacy.
ISO	TC 292	Security and resilience	Standardization in the field of security to enhance the safety and resilience of society. Excluded: Sector specific security projects developed in other relevant ISO committees and projects developed in ISO/TC 262 and ISO/PC 278.

6.3.1.2 Other initiatives related to regulation, guidelines and standardisation

In addition to the standards listed above, some regulations, guidelines, related initiatives, and documentation have been identified as potentially relevant by the EXERTER network. These are mentioned in short below.

- ADR regulations: ADR, formally the European Agreement of 30 September 1957 concerning the International Carriage of Dangerous Goods by Road[5], is treaty that governs transnational transport of hazardous materials.
- Pictograms, such as the Hazard Communication Standard Pictogram
- There are established systems for naming chemical substances. It is noted that countries could have their own system for naming chemicals (including many synonyms) which might lead to that some goods could be missed at controls due to the fact that synonyms are not checked. Relevant registers and identifiers for chemical substances are listed below.
    - CAS[6] Registry numbers
    - The EINECS[7]/ELINCS[8]/NLP[9] list in the EU Chemical Inventory that contains all phase-in or existing substances in Europe
    - UN numbers that are identifiers for dangerous goods and articles in the framework of international transport
    - IUPAC[10] names, used for naming organic compounds
- Different arrangements exist, such as The Wassenaar arrangement[11], on the topic of preventing the acquisition of conventional arms and dual-use technology by terrorists.

[5] https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XI-B-14&chapter=11&clang=_en

[6] CAS Registry number (also CASRN or CAS Number) is a unique numerical identifier assigned by the Chemical Abstracts Service to every chemical substance described in the open scientific literature.

[7] European Inventory of Existing Commercial Chemical Substances

[8] European List of Notified Chemical Substances

[9] No-longer Polymers

[10] International Union of Pure and Applied Chemistry

[11] "The Wassenaar Arrangement has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. The aim is also to prevent the acquisition of these items by terrorists. Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities." https://www.wassenaar.org/

- Additional initiatives related to the Prevent domain are the Chemical Weapons Convention[12] and the Australia group[13]. These cover chemical and biological weapons, but can be seen as related due to the fact that similar goods can also be used in case of explosives or in combination with them.

On the topic of markers, taggants, and control of explosives and detonators it has also been noted in the network that:

- There is EU Legislation regarding the labelling of detonators and explosives, which for example can be done with bar-coded stickers (Directive 2008/43/EC, Directive 2014/28/EU[14])
- In Northern Ireland for example[15] there is, in addition to implemented EU-regulations and the ADR treaty, extensive control of high explosives and detonators. This includes procedures with:
  - Police escort from point of entry to the quarry or mine etc. magazine;
  - Track & trace on the items, including a comprehensive requirement on logging out and accounting for use, destruction or return, from the commercial magazine by the mining company and overseen by the police
  - Trackers in vehicles carrying explosives components
- It is expressed that the legislation in relation to propellants/low explosive material is perceived as relatively relaxed, and to be more dependent on their ADR classification for transportation than the potential explosive characteristics. Stricter regulations regarding propellants/low explosives is noted as one potential possibility to reduce their accessibility.

6.3.2 Detect

6.3.2.1 Standardisation initiatives

A selection of standardisation initiatives and technical committees related the detection domain are listed in Table 5 below. There are also some standardisation initiatives that concern materials that could be of interest to the detect domain, e.g. CEN/TC 321 Explosives for civil uses. These have been excluded here but are presented in Table 4 (Prevent).

[12] "The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (the Chemical Weapons Convention or CWC)". "The Convention aims to eliminate an entire category of weapons of mass destruction by prohibiting the development, production, acquisition, stockpiling, retention, transfer or use of chemical weapons by States Parties. States Parties, in turn, must take the steps necessary to enforce that prohibition in respect of persons (natural or legal) within their jurisdiction." https://www.opcw.org/chemical-weapons-convention

[13] "The Australia Group (AG) is an informal forum of countries which, through the harmonisation of export controls, seeks to ensure that exports do not contribute to the development of chemical or biological weapons." "Coordination of national export control measures assists Australia Group participants to fulfil their obligations under the Chemical Weapons Convention and the Biological and Toxin Weapons Convention to the fullest extent possible" https://australiagroup.net/en/index.html

[14] Directive 2014/28/EU of the European parliament and of the council, of 26 February 2014, on the harmonisation of the laws of the Member States relating to the making available on the market and supervision of explosives for civil uses (recast) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0028&rid=8

[15] Procedures and legislation varies in the different EU countries

Table 5. Standardisation entities relevant for the counter-attack domain Detect

Entity	TC/WG	Name	Description
CEN	TC 391	Societal and Citizen Security	See Prevent
ISO	TC 292	Security and resilience	See Prevent
CLC	TC 79	Alarm systems	To prepare harmonized standards for detection, alarm and monitoring systems for protection of persons and property, and for elements used in these systems. The scope includes in particular intruder and hold-up alarm systems, access control systems, periphery protection systems, combined alarm - fire alarm systems, social alarm systems, CCTV-systems, other monitoring and surveillance systems related to security applications, as well as associated and dedicated transmission and communication systems. The standards shall specify conformity tests.
CLC	TC 216	Gas detectors	To standardize general and specific requirements for the construction, safety, performance and testing for electrical apparatus for sensing the presence of gas or vapour and for providing an indication, alarm and/or other output function, the purpose of which is to give a warning of explosion hazard, fire hazard or health hazard. The standardization work of TC 216 concerns domestic gas detectors and those industrial and commercial gas detectors that are not included in the scope of CLC/SC 31-9. To provide information and guidance, as appropriate, on the selection, installation and operation of such apparatus.

Existing standards for explosives detection, as listed by (Poustourli & Kourti, 2014), concern aviation and are: ECAC Common Evaluation Program for Security Equipment - Explosive Detection System; ECAC Common Evaluation Program for Security Equipment - Liquid Explosive Detection; and ECAC Common Evaluation Program for Security Equipment - Security Scanners.

6.3.2.2 Other initiatives related to regulation, guidelines and standardisation

In addition to the standards listed above, some regulations, guidelines, related initiatives, and documentation have been identified as potentially relevant by the EXERTER network. These cover in short surveillance, and standard procedures for manual searches and patrolling:

- Surveillance legislation is seen as a limiting factor when it comes to detecting IEDs in an urban environment. However, if technology was available and focussed, then it might be possible to use it within existing legal regulations in some situations.
- Based on threat analysis, security at train stations is for example increased for specific high risk events, prior to Cat 1 VIP visits, or following intelligence, e.g. with defensive search techniques. As a short-term measure, increased armed patrolling also occurs at high profile transport hubs.

A review of standards related to Explosives detection equipment is presented in the NDE[16] report "Requirements for the Implementation of a European Certification, Testing and Trialling Process for Explosives Detection" (NDE, 2011).

[16] Network on the Detection of Explosives

The work that has been performed by two ERNCIP thematic groups, one related to detection of explosives and one to video surveillance is noted as interesting. Their work is described in short below:

ERNCIP thematic group Explosives Detection Equipment (non-Aviation)[17]

“Since the 2006 transatlantic aircraft plot, the EU has defined legally binding technical specifications and performance requirement standards for various types of detection equipment used in EU airports, which call for European Common Testing Methodologies (CTMs) for detection equipment, to facilitate mutual recognition of approved or certified equipment. However, this kind of arrangement is not yet at the same maturity level for the detection of explosives outside the framework of aviation security e.g. for mass transport, special events, crowded places. There are different needs among the stakeholders, which hinders harmonisation, so it is currently not possible to propose a single scheme for the certification, testing and trialling of explosive detection equipment outside of aviation.”[17]

“Although definition of a common CTM for non-aviation security would be, at the moment, a too-challenging task for the ERNCIP TG, a common methodology that would evaluate the capabilities of the detection equipment (e.g. does it detect explosives?) and check the claims of manufacturers would be helpful, as it would provide an indicator to the potential of detection systems.”[17]

During 2013-2014 the Thematic group has produced the following deliverables:

- *Intermediate and final reports on non-aviation configurations with requirements for explosives detection - Statement of User Needs Final Report*: “This report for Task 1 of the ERNCIP DEMON Group, identifies user needs in the area of explosives detection for infrastructure protection applications (outside of aviation security). It spans guidance, training, equipment development, canine capability, and assurance, and considers various categories of infrastructure sites reflecting different detection needs.”
- *State of the Art report on existing regulations in Europe relating to the deployment of explosive detection equipment in non-aviation configurations:* “This report summarises European legislation relevant to explosive detection equipment, apart from that contained in the Aviation Security regulations. Although few other articles of European Union law directly refer to explosive detection, a number of directives and regulations are relevant to it, in the fields of explosives for civil use and pyrotechnics, dual-use equipment, chemicals and the chemical industry, port and inland transport security, and radiation, electromagnetic and electrical safety. Future European legislation in this field may be expected to conform to the principles of the EU’s New Legislative Framework, according to which harmonised standards are used to express detailed technical specifications. Current standardisation work is therefore also briefly described.”

ERNCIP thematic group Video Surveillance for Security of Critical Infrastructure[18]

“Recent years have seen a growth in the use of video surveillance technologies as part of the package of protective security measures used to protect critical infrastructures and other valuable assets. Academia and industry have been investing time and money in relevant technology innovations, but there is a lack of standardisation, testing and accreditation in Europe that would help users to ensure that video surveillance products are fit for their purposes.

This ERNCIP Thematic Group will endeavour to identify the activities at European level on video surveillance technologies within the security sector that will assist operators of critical infrastructure to improve their protective security.”[18]

[17] https://erncip-project.jrc.ec.europa.eu/networks/tgs/demon

[18] https://erncip-project.jrc.ec.europa.eu/networks/tgs/video

The focus in the 2015-2016 lifecycle was to:

- Determine how EU standards activities could best support user needs for the evaluation of video surveillance systems.
- Produce a guide for end users of factors to consider regarding the deployment of automated video surveillance.
- Determine how best to enable Collation/Common access to data sets in the EU for testing/evaluation of video surveillance software.

The following outputs:

- the options for a New Work Item relating to the use of video surveillance technology for security, and draft an outline roadmap that would eventually culminate in a Committee Draft Standard;
- a user guide for end-users of video security systems;
- a current state assessment on access to data sets in the EU for testing/evaluation of video analytics software and a gap analysis and recommendations regarding further development of access to data sets in the EU for testing/evaluation of video analytics software.

The report *Video surveillance standardisation activities, process and roadmap* (Ferryman, 2016) has been published.

6.3.3 *Mitigate*

6.3.3.1 Standardisation initiatives

A selection of standardisation initiatives and technical committees related the mitigation domain are listed in Table 6 below.

Table 6. Standardisation entities relevant for the counter-attack domain Mitigate

Entity	**TC/WG**	**Name**	**Description**
CEN	TC 129	Glass in building	Standardization in the field of glass used in building including: - definitions of all types of glass products, basic and processed; - definition of characteristics; - test methods for measurement of characteristics; - calculation methods for characteristics; - requirements e.g. durability; - classifications e.g. anti-bandit glazing; - glazing methods.
CEN	TC 263	Secure storage of cash, valuables and data media	Standardization in the field of physical security of products which provide secure storage of cash, valuables and data media in terms of resistance to fire and including high security locks.
CEN	TC 325	Crime prevention through building, facility and area design	Development of European standards for the prevention of crime at industrial facilities, educational institutions, hospitals, residential building areas, department stores, squares and public meeting places through building, facility and area design. The standards will include their area of application, the corresponding strategy, security levels, building and area layout, application of construction elements, roads and pavements. The standards may be applied to new and significantly refurbished buildings, facilities and areas. The standards will not deal with building products and security systems components.

CEN	TC 391	Societal and Citizen Security	See Prevent
ISO	TC 292	Security and resilience	See Prevent

6.3.3.2 Other initiatives related to regulation, guidelines and standardisation

The standard measures for mitigating effects of a terror attack in the public transportation varies, which could indicate a potential need for increased regulation. It is noted that in the UK, apart from the guidelines noted in Section 6.1, there are procedures for e.g. crowd control in place at larger train station hubs. There are restricted single points of entry to the platforms, where the commuter must pass a member of staff for ticket inspections, or regulated by a turnstile or barrier. Other implemented measures are that commuter trains in Great Britain often use separate confined luggage racks with partitions at the ends of the carriage to segregate passengers from large luggage (but does not assist with smaller back-packs etc.). The design of train carriages is also noted as an important factor for mitigating the effects from an explosion. This has been studied for example, after the 7/7 London bombings.

The "Reference Manual to Mitigate Potential Terrorist Attacks against Buildings FEMA-426/BIPS-06/October 2011" could be relevant for the mitigation domain.

Protecting Crowded Places: Design and Technical Issues, January 2012, Produced by the Home Office in partnership with the Centre for the Protection of National Infrastructure and the National Counter-Terrorism Security Office. This is a generic guide that gives advice about counter-terrorism protective security design. For example, it provides practical advice on how to "incorporate counter-terrorism protective security measures into proposed new development schemes whilst ensuring that they are of high design quality".

ERNCIP thematic area "Resistance of structures to explosion effects": Thematic group on the resistance of structures to explosion effects. Formed in order to bring the required expertise together, make it commonly available and to find and define harmonised methods and solutions, which can be provided to the decision-makers responsible for critical infrastructure protection.

Each EU member state Police unit has internal Standard Operating Procedures for mitigation.

6.3.4 React

6.3.4.1 Standardisation initiatives

A selection of standardisation initiatives and technical comities related the detection domain are listed in Table 7 below.

Table 7. Standardisation entities relevant for the counter-attack domain React

Entity	TC/WG	Name	Description
CEN	TC 239	Rescue systems	To define standards for emergency for emergency medical vehicles and the equipment thereof as well as for first aid equipment, in the interests of providing safe and comfortable transport and preclinical treatment for patients.
CEN	TC 391	Societal and Citizen Security	See Prevent
ISO	TC 94	Personal safety -- Personal protective equipment	Standardization of the performance of personal protective equipment designed to safeguard wearers against all known possible hazards.

ISO	TC 292	Security and resilience	See Prevent
CLC	TC 79	Alarm systems	See Detect
ISO	IEC 17025	Testing and calibration	General requirements for the competence of testing and calibration laboratories, this is the main ISO standard used by testing and calibration laboratories. In most countries, ISO/IEC 17025 is the standard for which most labs must hold accreditation in order to be deemed technically competent.

6.3.4.2 Other initiatives related to regulation, guidelines and standardisation

The European Network of Forensic Science (ENFSI) have guidelines for the gathering of evidence[19]. It is noted that there are national protocols for post incident response.

The US Department of Transportation has published, and continually updates, an Emergency Response Guidebook[20]. PHMSA's 2016 Emergency Response Guidebook provides first responders with a go-to manual to help deal with hazmat transportation accidents during the critical first 30 minutes. It is a guidebook intended for use by first responders during the initial phase of a transportation incident involving dangerous goods/hazardous materials."

Related to the react domain, a selection of procedures implemented in the UK have been noted by the EXERTER network. These are described below:

The UK standard Joint Emergency Services Interoperability Programme (JESIP) is a joint doctrine that was developed to improve and standardise the way the police, fire & rescue, and ambulance services work together when responding to major multi agency incidents in the UK. This doctrine will be invoked when any major incident occurs, and will ensure a prioritised and effective method of command and control, plus inter agency communication. JESIP have also produced a publicly available App. Other procedures in place include:

- protected identified phone numbers to form a ring-fenced strategic network in the event of the collapse of the general phone network following a major incident;
- the holding of regular joint agency exercises and training to prepare for the aftermath of a major incident;
- and in Northern Ireland, in the event of a major explosive incident, tried and tested procedures are in place where the military EOD will make safe a scene, and experienced Crime Scene Forensic Managers will coordinate appropriately trained CSIs to secure and collect evidence, with the option of calling on forensic scientists from the Forensic Service Northern Ireland for support.

There are also, in the UK mainland, dedicated telephone numbers for commuters to contact for left luggage or suspicious behaviour at key transport hubs. Frequent Counter Terrorism overt patrolling is also used. In addition, other Government Social Media campaigns, and Apps[21] designed to prepare the general public for catastrophic events (as well as aide memoir on what to do post attack) are also available.

[19] http://enfsi.eu/documents/best-practice-manuals/

[20] https://www.phmsa.dot.gov/hazmat/erg/emergency-response-guidebook-erg

[21] such as the CitizenAid app

7 Exploitation support

7.1 Introduction and overview

Technology and tools are central in countering the terror threat and bridging the practitioners' gaps and requirements (see Section 4). Thus, EXERTER works with finding appropriate state-of-the-art technology in the field of SoE, and focuses on supporting collaboration and interaction between different actors to improve exploitation possibilities.

Supporting collaboration and exploitation in the SoE field is achieved through creating a link between academia, industry, researchers and end users. These links will help to exploit new research and facilitate the process of taking final steps towards commercialization (Researcher vs End-user needs vs Industry vs Academia).

7.2 Market screening and state-of-the-art technologies

EXERTER performs a market screening of equipment used within security of explosives. A first draft of a generic overview of the state-of-the-art technologies has been defined, where the equipment is categorised and the important key elements are highlighted. The level of detail is higher for some of the relevant sub-categories in the list.

EXERTER has also been granted access to a database with emerging counter tools, collected within the H2020-project ENTRAP. Discussions on how to use and possibly restructure this database for the needs of EXERTER are ongoing.

7.3 Support for collaboration and exploitation

EXERTER has started a dialog with companies, academia and research institutions, and are performing surveys and interviews. Until March, interviews had been conducted with five different institutions; EXPAL/ MAXAM (Industry), Escribano (Industry), BR Line (Industry), Escuela Técnica Superior de Ingenieros de Minas y Energía (Academia), and INTA (R&D center). Surveys and interviews will be performed continually.

During the interviews, the organisations' products and work areas are documented (connected to the counter attack domains) and a selection of topics are discussed. Topics are for example; obstacles and drivers for innovation, regulations that hinder their R&D, situations that drives/encourages their R&D, and what is missing in terms of technology, standards, information, communities for their development and research. The interview forms are provided in full in Annex 1.

Work with collecting summarised information about relevant companies, universities and research organisations, along with their research, R&D in specific fields, and fields of application, is ongoing. This will give a holistic view of the current technology situation for the SoE (prevention, detection, mitigation and reaction).

During the interviews, the need for knowing practitioners' needs and requirements in terms of security/SoE products was highlighted by the companies. A continually updated list[22] with needs, where they can check the current tenders in the public procurement platforms belonging to Police, Law Enforcement, Intelligence and Defence, was suggested as a way to support the companies' work and R&D activities.

[22] Requested by an interviewee to be "An overall description of the main necessities with a point of contact where enterprises could have their calls answered in English, and the URL where they can check the current tenders in the public procurement platforms belonging to Police, Law Enforcement, Intelligence and Defence."

Regarding regulation barriers that prevent research or development activities, one organisation pointed out that*: "In the financing R&D activities field, we find a barrier in the complexity of the administrative procedures. The simplification or unification of the procedures will help to improve companies' effort on R&D."* There is thus a need for a straightforward procurement procedure in the administrations. This starts with a clear declaration of practitioners' needs, and communication of these to the companies, so they can focus their development and manufacturing efforts in the right direction.

8 Analysis and recommendations

8.1 Overview

In the following sections, Section 8.2 to 8.5, preliminary analysis and recommendation is provided in relation to the second yearly scenario, the public transportation scenario. Any potential update will be provided in future deliverables, either in D6.5 or D6.6, depending on when in time the 2nd EXERTER conference can be held.

8.2 Prevent

For the 2nd yearly scenario, the prevent domain is focused on commercial explosives. Hindering the access to commercial explosives and other IED components, as well as detecting and identifying them are therefore been the main aspects that have been considered.

Access to explosives can primarily be regulated through legislation and control, and the relevant regulations at EU-level are covered by e.g. Directive 2014/28/EU[23], Directive 2013/29/EU[24] and Directive 2008/43/EC[25]. However, it is noted that legislations, implemented procedures and control of explosives for civil use varies between different EU member states. Increased regulatory actions, preferably at an EU-level, could be one alternative for reducing the amount of stolen explosives, and their illicit use. It is also important that procedures, controls and actions aim to cover the entire chain of transport, storage and use of the explosive, to prevent weak links.

Part of the EU-regulations considers identification and tractability of explosives for civil uses. The requirement[25] is to have adhesive labels, or printed information on the packaging. To introduce permanent markings on e.g. detonator bodies may be one solution that that could assist improved traceability. This could for example be achieved through impressing or etching a QR type code into the body, prior to their assembly with energetic contents.

The carriage of hazardous substances is addressed in the ADR[26] treaty. The ADR treaty contains security aspects[27] and lists some general provisions to minimise theft or misuse of the transported goods. High consequence dangerous goods (meaning those with potential misuse in a terrorist event) are specified as a special category in the security provisions and these goods requires additional security plans. The security aspects for carrying dangerous goods could be an area for further study, particularly with regard to explosives not listed as high consequence dangerous goods.

Regarding the detection and identification of substances, there is a possibility to add markers for detection (pre-attack) and taggants for identification of explosives (post-attack) in commercially produced explosives. Today, Switzerland is the only country that requires identification taggants, in the form of coded polymers, to be incorporated into the explosive substances.

[23] Directive 2014/28/EU of the European parliament and of the council, of 26 February 2014, on the harmonisation of the laws of the Member States relating to the making available on the market and supervision of explosives for civil uses (recast) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0028&rid=8

[24] Directive 2013/29/EU of the European parliament and of the council of 12 June 2013, on the harmonisation of the laws of the Member States relating to the making available on the market of pyrotechnic articles (recast) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2013.178.01.0027.01.ENG

[25] Directive 2008/43/EC of 4 April 2008. Setting up, pursuant to Council Directive 93/15/EEC, a system for the identification and traceability of explosives for civil uses. Covers the identification and traceability of explosives.

[26] Agreement concerning the International Carriage of Dangerous Goods by Road

[27] See ECE/TRANS/275 (Vol.I), Chapter 1.10

Detection markers are substances that could enhance the possibility to detect the explosive with explosives detection dogs or technical devices. Due to the convention on the marking of plastic explosives[28], many countries require markers to be added to these explosives. The convention is currently ratified by 155 states that then prohibits the manufacture, storage, transport or entry of any unmarked explosives on their territory. The substances that are allowed to be used as markers (specified in an annex to the convention) are volatile substances whose molecules exist in a higher concentration than the explosive substance itself around the explosive. Explosives detection dogs are trained to identify these markers. However, to assure that all dogs can detect explosives with varying degree of marker present, a need for commonly used guidelines regarding the handling of substances used in the training of dogs has been identified.

Systems with taggants for identification and markers for detection might be one piece for aiding the prevention of certain incidents with theft and illicit use of commercial explosives. Research on different types of markers to be incorporated into explosives for civil use and explosives precursors could be one way of improving the possibility to detect explosives for illicit use.

If measures such as using identification taggants and detection markers should have good effect, it is suggested that that they should be widely adapted across EU, integrated with the development of detection equipment (for detection markers), and consider a wide range of societal perspectives.

8.3 Detect

Detection of terrorists or IEDs on or within a public transportation system requires detection systems that can scan a large number of people, preferably in free flow and without the need for any divesting. This poses technical challenges as well as highlights the need for a holistic approach to find suitable solutions. Another important aspect to consider is how to proceed after a potential threat have been identified. This to be able to neutralise the threat, or mitigate the consequences of the attack.

To improve the security of public transport against terrorist attacks it is important to review existing security policies, procedures and technologies, and identify gaps and proposed targeted solutions. There is a lack of consistency in terms of the provision of security across the EU and there is no overarching security policy at the European level in this sector, for daily themes such as the organisation of security, information management, and video-surveillance. There are/have been some European initiatives with the aim to increase harmonisation of certification and standardisation in the area. For example, efforts to map the needs were pursued by the ERNCIP thematic groups.

It is important to develop a generic methodology for risk assessment for public transport systems and there is a need to raise awareness of the risks among users of public transport. Harmonised risk-analysis methodologies should be used to prioritise possible detection actions and to ensure that the measures introduced would be cost-effective. Only after a coherent and standardised analysis of the risks and hazards that are faced by public transportations, is it possible to develop a common agreed process and layout for detection systems.

The design of new stations and the renovation of existing ones, including the design of its interior and the design of associated services, should also be taken in consideration to improve the detection aspect. At this stage, a roadmap can be developed for the most promising integrated solutions for addressing the security of passengers using mass public transport.

In the recent years, the approach or the management of passenger security checks in train stations is following somehow the design of airport check-in areas. It could prove beneficial to take similar approaches to the design, implementation and evaluation of different aspects of the security surrounding all passenger transport modes even if, this type of approach is difficult to apply to situations that are

[28] The 1991 International civil aviation organisations convention on the marking of added to plastic explosives for the purpose of detection

faced by the most crowded train stations. Mass public transportation faces similar threats of an airport but is less easy to counter as a result of the higher number of access points, higher frequencies of use and shorter journeys. For the counter attack domain detect it might not be easy, technically or economically, to replicate the security arrangement for air travel.

For this reason, there is still a need of development and testing of technologies for public transportation, which can be used to facilitate improved security without interfering with the normal flow of passengers. The most innovative approach to pursue, like those already suggested in some NATO and European projects, is one that foresees the application of a system of systems to detect remotely and in real time, without disrupting the flow of passengers and with a reduced level of false alarms, the presence of a terrorist threat. There is a need for development of scanning technologies suitable for use on public transport, at stations and on-board vehicles, without generating inconvenience for passengers.

The implementation and use of improved CCTV (behavioural analysis, facial recognition) on public transport vehicles and at public transport stations for the purposes of security should also be pursued. Intelligent video systems could be deployed to locate and track people with suspicious behaviour or appearance at a certain distance for further detection. Use of facial recognition technology, or proximity technology, could also allow for notification to law enforcement when a number of known or suspected terrorists congregate in a transport hub together in close proximity at one time. For the analysis of the computed trajectories with respect to anomalies, it is necessary for the system:

- to have a definition for, or to learn, suspicious and non-suspicious behaviour
- to be able to perform computation and analysis of trajectories over a camera network

The use of cameras for the detection and tracking of objects in a flow can be an important information source either in the analysis of the behaviour (trajectories) of relevant objects or in combination with detectors of explosives to generate live alarms.

Another potential approach is the use of a sensor network that is able to collect data about the environment where they are operating (buses, trams, underground and light rail systems) and, communicate this in real-time to a security management centre.

The ideal detection would be fast, accurate, work from long distances, be safe for people, able to detect threats through clothing or other masking devices with low false alarm rate and high probability of detection but, at the moment, a single sensor is not able to satisfy all these characteristics well enough to be used as a stand-alone system. Thus, there is the need of the implementation of an integrated protection system, and, at the same time, the detection of a threat should be based on both the behavioural anomalies of people and on the properties of the IED (chemical and physical properties, design, dimension, etc.). All the information acquired should be merged together in a more complex smart decision data fusion in order to enhance the detection performance.

Research is needed on the integration of information from distributed orthogonal sensors to achieve real-time conflict resolution and decision making with high system effectiveness, and on integration tools based on data fusion and decision fusion. In addition, research coupling parallel sensors via decision fusion with sequential sensor systems may provide valuable insights. Some technical challenges related to the implementations of such architecture are for example:

- How and time to get valuable information (sampling);
- Data transfer;
- Communication between sensors;
- Fusion of information;
- Detection decision making;
- Deployment issues; and
- Sensor fault detection;

8.4 Mitigate

Several research initiatives already addressed aspects of possible mitigation measures related to the effects of a terrorist attack on (or within) a public transport system. Potential mitigation measures in such environments are related to (i) organisational/management measures, as addressed e.g. in SinoVE Management, (ii) the structural design of passenger stations as addressed in SECURESTATION, (iii) the design of the means of transport as addressed e.g. in SECUREMETRO and (iv) innovative sensor technologies that could help to early detect suspicious situations, as developed in Sense4METRO.

Standardisation initiatives that might be relevant for attacks on (or within) public transportation vehicles are related mainly to structural components, as glass (CEN, TC1299) and, in a wider sense, the design of buildings, sites and urban areas against criminal attacks and the management of transport facilities (e.g. CEN TC263 and 325). However, terrorism is not specifically included in these standards and, hence, their specific characteristics are not addressed.

Despite the progress of the research initiatives and technology developments on the design and structural properties of public transportation and passenger stations, the MITIGATION of explosion effects for the given scenario is challenging. The scenario, an attack on commuter trains in a metropolitan area, is characterized by a large number of people on confined spaces as well as the explosion influenced by the confinement of these spaces. Related to these characteristics, future research initiatives and technology developments on the structural or design side should look at:

- Venting openings in trains, that effectively reduce overpressure conditions inside the train following an explosion
- Separated luggage compartments, with basic protection measures in passenger directions (stable design, no fragmentation possible)
- Design train interiors in order to prevent hazardous fragmentation of structural components
- Design train windows to prevent fragmentation, e.g. to protect people in metro/train stations from in train explosion effects – or the other way around.
- Design of metro/train stations to: minimize fragmentation, increase early venting openings, protect bearing columns to avoid structural collapse, instalments to generate safe protected areas reducing blast effects between adjacent zones, and avoid large crowds
- Further development of IED neutralisation techniques

Furthermore, research on organizational measures is suggested regarding:

- Measures that reduce congestion in train/metro stations
- Evacuation concepts in case something suspicious is detected
- Training of train crews, train station staff and first responders (police, firefighters, ambulance, bomb squad) with respect to fast evacuations, care about injured persons, prevent further attacks and IED neutralisation.

Despite past, recent and future research initiatives and technology developments addressing the mitigation of explosion effects on public transport systems, the success of these measures can only be limited. Many of them would either require considerable monetary efforts (i.e. to build every train blast resistant) or are almost inapplicable or even impossible (i.e. to avoid crowds in transport systems in metropolitan areas during peak hours). Thus, especially the organizational measures are highlighted and suggested as a field of future research, as their implementation is most likely, compared to design/structural measures, easier and more cost effective.

8.5 React

Work on standardization and certification regarding national and international procedures in the field of law enforcement, evidence gathering and post-blast work is still needed to work together at bigger attack sites. This is of course important on a national basis but even more so on an international (EU) basis, as attacks like the Madrid bombings, can easily overwhelm the resources of many countries. Especially the number of specialized Explosives crime scene officers needed to resolve such scenes.

Even if information exchange regarding explosive incidents within the EU is on the right track to be done routinely through the bomb data centres, reaction and help by case officers in an emergency is not done routinely. This type of help can only seriously be offered and accepted if both agencies have the same standardized protocol of work at those scenes. Obviously, this would require an international (EU) certification system to ensure that the officers called to the scene produce evidence of such quality that they are valid in court. There are some projects working to ensure that the training of crime scene officers is up to date within the EU.

This approach would be equally useful if a similar certification / standard training system could be used on a national level for first responders, getting them used to explosive attack sites.

Certifications targeting the reduction of risks, regarding the handling of hazardous chemicals are already in progress in several EU-States. This includes guidelines and requirements for warning systems, as well as better personal protective equipment for instance. First steps are made with the Standing committee of precursors in regard to a standardized warning system for precursors for HME production.

In addition, the monitoring of hazardous substances that is already in use has to be expanded continuously in connection to the use of HME in IED. Here simple and easily accessible information for sellers and first respond security forces needs to be included.

It also has to be checked if precursor substances could be phlegmatised or inhibitors added to make them unusable for HMEs. This is typically more effective than simple prohibition, as this would make theft or buying those substances in disguise with the intention of HME production much more difficult. Analogically with this, the reliability and possibility of track and trace of commercial and military ammunition and explosives has to be improved steadily and brought to a standardized level at least within the EU.

As shown in the scenario and all research made in this topic, critical infrastructure is still not hardened to cope with such an incident. Especially phone and computer networks have to be modified and stabilized to avoid a collapse in the aftermath of a terrorist attack of such a scale. Nevertheless, there are several research projects that deal with the topic of adjusting and improving the existing norms and crisis management on a local and international level. The results have to be reviewed if they are applicable at the national level.

There is considerable progress noticed regarding the growing number of projects and techniques dealing with the surveillance of public spaces. The possibilities of controlling areas, people and baggage in context with public transport systems have perceptibly improved, just as the quality of CCTV pictures has increased. At the same time, many of the projects also mention the data security aspects of such measures. The results are envisioned to help the direct response at the time of the incident but also in the later react phase to help the forensic investigation.

The research in the area of stand-off detection of hazardous substances and explosives as well as in the field of forensic analysis is still conducted to a high degree. These includes techniques to determine secondary devices in the mitigate/ react phase but also in the pure sense of forensic evidence gathering and analysis to build field labs which could produce court relevant information. The implementation of these techniques into best practice manuals or standardized procedures can nevertheless not be observed. This might be due to the lack of commercially available systems. The reason for the lack of these systems produced being that police- and forensic end users are still a very small market which do not justify large investments.

Finally, all measures that are taken as a result of research or as a reaction after an attack need to be transferred into standard operating procedures in the post-blast work and everyday routine. This typically takes quite a long time with large organization especially security conscious ones.

9 References

(Burton and Stewart, 2008): Burton, F., and Stewart, S. (2008). The ‘lone wolf’ disconnect. Terrorism Intelligence Report-STRATFOR. Retrieved from https://worldview.stratfor.com/article/lone-wolf-disconnect

(CPNI, 2017) Centre for the Protection of National Infrastructure, *Protecting against terrorism,* Third edition, Centre for the Protection of National Infrastructure (CPNI), 2017

(Das, 2016): Das, R. (2016). The burden of insecurity: Using theories of International Relations to make-sense of the state of post-9/11 politics. Relationsinternational.com.

(DoT, 2012): Department for Transport. (2012). Security in Design of Stations (SIDOS) Guide, Department for transport

(DoT, 2014): Department for Transport. (2014). Light Rail Security - Recommended Best Practice. Department for transport

(DoT, 2018): Department for Transport. (2018). Bus and Coach Security - Recommended Best Practice. Third edition. Department for transport

(Ellis, 2016): Ellis C., Pantucci R., van Zuijdewijn J. R., Bakker E., Gomis B., Palombi S. & Smith M. (2016). Countering Lone-Actor Terrorism Series No. 4. Lone-Actor Terrorism Analysis Paper. Royal United Services Institute for Defence and Security Studies.

(European Parliament, 2018): European Parliament. (2018). The return of foreign fighters to EU soil: Ex-post evaluation. European Parliamentary Research Service

(Europol, 2016): Europol (2016). Changes in modus operandi of Islamic State terrorist attacks. Review held by experts from Member States and Europol on 29 November and 1 December 2015. Europol Public Information.

(Europol, 2019a): Europol. (2019). TE-SAT 2018: EU Terrorism Situation and Trend Report. Publications Office of the European Union.

(Europol, 2019b) Europol (2019). Do Criminals Dream Of Electric Sheep? How Technology Shapes The Future Of Crime And Law Enforcement. Publications Office of the European Union.

(Ferryman, 2016): Ferryman, J. (2016). Video surveillance standardisation activities, process and roadmap. ERNCIP Thematic group video surveillance for security of critical infrastructure. JRC.

(Ganor, 2015): Ganor, B. (2015). Global alert: The rationality of modern Islamist terrorism and the challenge to the liberal democratic world. New York: Columbia University Press.

(Hoffman, 2006): Hoffman, B. (2006). Inside terrorism. New York: Columbia University Press.

(Jones 2018): Jones, S. G., Toucas, B., & Markusen, M. B. (2018). From the IRA to the Islamic State: The evolving terrorism threat in Europe. Center for Strategic & International Studies.

(Joosse, 2007): Joosse, P. (2007). Leaderless resistance and ideological inclusion: The case of the Earth Liberation Front. Terrorism and Political Violence, 19(3), 351-368. doi: 10.1080/09546550701424042.

(Mockaitis, 2007): Mockaitis, T. R. (2007). The" new" terrorism: myths and reality. London: Greenwood Publishing Group.

(NaCTSO, 2017): National Counter Terrorism Security Office. (2017). Crowded Places Guidance. NaCTSO

(NDE, 2011): Network on the Detection of Explosives. (2011). Requirements for the Implementation of European Certification, Testing and Trialling Process for Explosives Detection, Network on the Detection of Explosives EU Contract JLS/2008/ISEC/PR/020-D1

(Neumann, 2016): Neumann, P. R. (2016). Radicalized: new jihadists and the threat to the West. Bloomsbury Publishing.

(Poustourli & Kourti, 2014): Poustourli, A., and Kourti, N. (2014). Standards for critical infrastructure protection (CIP) - the contribution of ERNCIP, JRC

(Rapoport, 2002): Rapoport, D. C. (2002). The four waves of rebel terror and September 11. Anthropoetics, 8(1), 1-17.

(SBD, 2020): Secured by Design. (2020). Resilient Design Tool for Counter Terrorism, version 3.21, accessed: 2020-05-25, https://www.securedbydesign.com/images/downloads/resilient-design-tool-for-counter-terrorism.pdf

(Simon, 2000): Simon, S. and Benjamin, D. (2000). America and the New Terrorism. Survival, 42(1). 59-75.

(Tucker, 2001): Tucker, D. (2001). What is new about the new terrorism and how dangerous is it?. Terrorism and Political Violence, 13(3). doi: 10.1080/09546550109609688.

(UIC, 2013) International Union of Railways. (2013). Human factors - Preventive measures against terrorist act on railway premises, and Guidelines for managing suspicious items in railway premises. International Union of Railways.

(UIC, 2017): International Union of Railways. (2017). Station security for station business - Handbook on effective solutions. International Union of Railways.

(UIC, 2019a): International Union of Railways. (2019). UIC Security Platform - Human Factors - Guidelines for managing suspicious items in railway premises for rail passengers and visitors. International Union of Railways.

(UIC, 2019b): International Union of Railways. (2019). UIC Security Platform - Human Factors - Guidelines for managing suspicious items in railway premises for railway staff. International Union of Railways.

10 Abbreviations and Definitions

ADR	Accord Européen Relatif au Transport International des Marchandises Dangereuses par Route på franska eller European Agreement Concerning the International Carriage of Dangerous Goods by Road
CBRN	Chemical, Biological, Radiological and Nuclear
CCTV	Closed-Circuit TeleVision, video surveillance
CEN	European Committee for Standardization
CENELEC CLC	European Committee for Electrotechnical Standardization
D	Deliverable
EC	European Commission
EEC	End user and Expert Community, external group of stakeholders in the field of SoE which have agreed to support and interact with the EXERTER consortium
FTF	Foreign Terrorist Fighter
HME	Homemade Explosive
IED	Improvised Explosive Device
ISO	International Organization for Standardization
LEA	Law Enforcement Agency
M	Month since project start
MENA	Middle East and North Africa
MS	Member State
QR	Quick Response
R&D	Research and Development
SoE	Security of Explosives
UAV	Unmanned Aerial Vehicle
WP	Work Package

Disclaimer:
The content of this report reflects only the author’s views and the European Union is not liable for any use that may be made of the information contained herein.