17/03/2020

Version no. 2.1

EXERTER

Security of Explosives pan-European Specialists Network

D6.2
2nd Report on Innovations, Standardisation and Exploitation within SoE

FOI
ENEA
KEMEA
FhG-EMI
BKA
FhG-ICT
ICPO
INTA
NEN

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

D6.2
2nd Report on Innovations, Standardisation and Exploitation within SoE

Main Authors	
Name	*Organisation*
Matilda Ågren	FOI
Patrik Krumlinde	FOI
Roberto Chirico	ENEA
Ioannis Daniilidis	KEMEA
Johannes Schneider	FhG-EMI
Malte von Ramin	FhG-EMI
Ansgar Japes	BKA
Erik Plessinger	BKA
Ian Tippett	ICPO
Carlos López Pingarrón	INTA
Miguel Angel Ropero Azañon	INTA
Lara Hettmanczyk	FhG-ICT
Frank Schnürer	FhG-ICT
Christian Ulrich	FhG-ICT
Okke-Jaap Prent	NEN
Ronald de Boon	NEN
Contributors	
Anneli Ehlerding	FOI
Ola Norberg	FOI

Document information		
Version no.	*Modification(s)*	*Date*
v. 1.0		31/05/2019
v.2.0	Corrected the dissemination level to PUBLIC	19/09/2019
V2.1	Removal of annexes from main report	17/03/2020

Summary

This document is the second 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.

This deliverable summarises and analyses the findings on innovations, standardisation and exploitation from WP2, WP3, WP4 and WP5 related to this year's scenario: the July 22nd 2011 bombing in Oslo, Norway. The aim is to produce tangible and useful output for all SoE stakeholders.

Three unclassified annexes are connected to this report. D6.2 Annex 1-3 are consortium confidential and contains tables with Overview of research projects, Standardisations, full list and Technologies.

Two classified annexes are connected to this report, D6.2 Annex 4 and D6.2 Annex 5. Annex 4 contains identified requirements and gaps related to this year's scenario and Annex 5 is the analysis related to the counter attack domain prevent. Annex 4 is security classified EU Restricted and Annex 5 is security classified EU Confidential.

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 in order 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 in order 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, content of the report and delimitations

This report is the second of the 6-monthly Deliverables on analysis and recommendations in the EXERTER project. It aims at summarising information on innovations, standardisation and exploitation based on the findings of WP2, WP3, WP4 and WP5 related to the yearly scenario. This year's scenario was the July 22nd 2011 bombing in Oslo, Norway. The scenario and its specific key elements, connected to each counter attack domain, are described in the EU-restricted D6.1 Annex 1.

The scenario is used as a framework to highlight different aspects of the explosives threat, and work with the aspects within research and innovation, standardisation and exploitation. Four different counter attack domains are continuously pursued for the yearly scenarios and the activities: Prevent, Detect, Mitigate and React, see Figure 1.

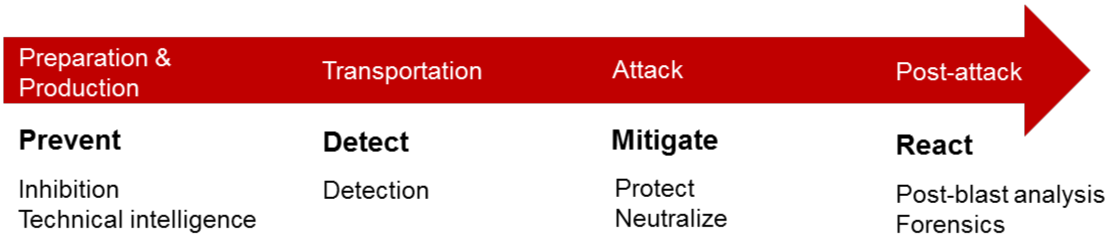


Figure 1: The counter attack domains addressed by EXERTER as identified prior to project start.

The content of this report is made up by the internal deliverables from WP2, WP3, WP4 and WP5, along with input and analysis from task leaders and partners in WP6. The report connects and combines the findings from the different areas in EXERTER related to the first yearly scenario, the 22nd July 2011 Oslo bombing. Key elements in the scenario were highlighted in D6.1 Annex 1. These have been studied from different angles and the outcome is summarised in this report. Related to the yearly scenario and the identified key elements, this report illuminates requirements and gaps (Annex 4), provides an overview of ongoing and finished research projects (Section 3), summarizes findings on standardisation, certification and regulation (Section 4), and gives a review of products and exploitation efforts (Section 5). The analysis and recommendations provided by the task leaders in WP6 are presented in Section 6 and Annex 5, and comments on future work are made in Section 7. The results from this report will be disseminated externally to the wider SoE community through WP7 and WP8.

Two security-classified annexes, Annex 4 and Annex 5, are connected to this report. Annex 4 reports on the requirements and gaps related to the yearly scenario and is classified Restreint UE/EU Restricted. Annex 5 is the analysis and recommendation related to the counter attack domain Prevent. This annex is classified Confidentiel UE/EU Confidential.

1.3 Scenario in brief

For quick orientation, this section gives a brief overview of the July 22nd 2011 bombing in Oslo, Norway. The information is parts reprinted from the WP2 scenario description, which in turn was based on information from open sources, e.g. the report from the independent investigation of the attack and societal response “Rapport fra 22. juli kommisjonen”[1], and Breivik’s manifesto[2], which is still available online.

On 22 July 2011 the perpetrator, Anders Behring Breivik, detonated a Vehicle-Borne Improvised Explosive Device (VBIED) in Oslo, Norway, killing eight people. The bomb contained a large quantity of Explosive (HME), made from precursor chemicals he had obtained from various sources. Breivik then went on to shoot 69 people on the island of Utøya, but this is not within the scope of EXERTER.

A detailed review of the scenario was undertaken by an Independent Commission appointed by the Norwegian government. It highlighted a number of issues and areas of concern, which have now been resolved, and they indicated that there were areas where early intervention could have prevented these deaths. The report concluded that Breivik’s success was due to his determination and a measure of luck. This particular plot is interesting, partly since Breivik was able to obtain relevant precursor chemicals, manufacture and detonate the bomb in Oslo, which breached a number of laws and regulations designed to prevent this from happening.

1.3.1 Planning

The planning of the attack is seen to start four years prior to the attack. Breivik then started his online research and began writing his manifest. Two years later, Breivik started to acquire equipment, bought a farm situated 160 km north of Oslo where he later produced the bomb, and registered his business, Breivik Geofarm ENK.

1.3.2 Pre-attack

At 9 months prior to the attack, Breivik began to acquire chemicals and equipment for bomb production. He bought fertilizer, diesel, nitromethane, sodium nitrite, aluminium powder, sulphuric acid, sodium nitrate and 2-3 packages of aspirin from 20 different pharmacies in Oslo. He also acquired 15 metres of

[1] Norges offentlige utredninger (NOU) 2012:14, “Rapport fra 22. juli kommisjonen”. The report can be downloaded from https://www.regjeringen.no/no/dokumenter/nou-2012-14/id697260/ (accessed 2018-07-05).

[2] The manifesto can be downloaded from multiple sites, for example (accessed 2018-07-05):
https://info.publicintelligence.net/AndersBehringBreivikManifesto.pdf
http://www.democratie.ulg.ac.be/wp-content/uploads/2013/01/Breivik-Manifesto.pdf

hobby fuse over the internet. Breivik could operate undisturbed at his remotely located farm. About 2.5 months prior to the attack, he began to synthesize the needed homemade explosives and to mix the materials for the bomb. He concentrated sulphuric acid, grinded the fertilizer to make ANFO, synthesised picric acid and DDNP from acetylsalicylic acid, mixed ANFO with aluminium powder and concentrated nitromethane. He was finished two days prior to the attack.

1.3.3 Attack

The car with the bomb (approximately 950 kg ANALFO, Picric Acid (200-300 gr), DDNP (10 gr)**,** Nitromethane (unknown amount)) was parked twenty minutes from the bombsite the day before the attack. An escape car was placed strategically. On the day of the attack, at 15:17 he parked the car with the bomb outside the government building. He ignited the bomb fuse and left the vehicle, which exploded after seven minutes.

1.3.4 Post-attack

Police patrols arrived at the scene of the attack after 5 minutes and the task force leader arrived 4 minutes later. He concluded, based on the damages, that the main charge likely had went off and it was unlikely that any further bombs were present. The rescue work was initiated and a coordination site for ambulance personnel and injured people had been set up 12 minutes after the attack.

Only 10% of the people working in the government building was present in the building at the time of the attack. Eight people were killed. Buildings up to 500 meters from the blast scene were damaged in the attack. No buildings collapsed.

2 Identified requirements and gaps

The identified requirements and gaps are provided in an EU Restricted annex, Annex 4, to this report. The information in the annex is a summary and analysis of input received from stakeholders concerning requirements and gaps connected to security of explosives capabilities.

A questionnaire was used to collect expert knowledge on requirements and gaps related to the first of the yearly scenarios, and to highlight methods to prevent, detect, mitigate and/or react to similar attacks. The questionnaire was sent to individuals in the Security of Explosives community, some members of the EXERTER End user and Expert Community and to other practitioners.

The information in Annex 4 is based on a combination of the answers provided to this questionnaire along with the responses to questions posed in a Table-Top Exercise run during the EXERTER workshop in Rome. Highlighted are also some areas that are believed to be the most important to work with within the respective counter attack domain.

Practitioners' ideas and knowledge on requirements and gaps will support the continued work in EXERTER. In order to ensure that the received information is relevant to the scope of the project the task leaders will be further involved in the process of constructing the future questionnaire, and in holding the workshops.

Some highlighted aspects of the scenario are also discussed in EXERTER D6.1 Annex 1. The information therein was used support the discussion and analysis during the first EXERTER End User Workshop in Rome. The outcome from the workshop is reviewed in Section 2.2 in D6.2 Annex 4.

3 Research review

3.1 Introduction

In EXERTER, a research review identifies and collects information from national, European and international research projects related to Security of Explosives (SoE), which can help in the fight against terrorism. Both ongoing and completed projects are considered.

To give an overview of SoE research activities, research and innovation, projects are continuously assessed through literature surveys, interaction and communication with other research projects, web searches and interviews. The identified projects are compiled in an Excel sheet, which is described in Section 3.2 and presented in Annex 1. From the general overview in the Excel sheet, a number of projects with relevance for the first yearly scenario have been highlighted and further assessed. A preliminary list with the highlighted research projects is presented in Section 3.3 below.

3.2 Overview of SoE Research Activities

Based on overviews from other projects, for example ENTRAP, NDE and HECTOS, and further publicly available summaries (e.g. webpage of projects, CORDIS search, databases), an overview of SoE research activities have been compiled in an Excel table. Important key elements have been specified to include the most relevant information in a generic overview. These are defined as follows:

- Project/publication short name
- Project full name, publication title etc.
- Grant
- Topic/summary
- Project duration
- Website
- Relevance - Counter Attack Phases
- Relevance to the Scenario of the year 1: Oslo bombing
- Developed Tools: Categories
- Developed Tools: Description
- EXERTER-partners involved
- Comments

The relevance of the listed research projects for each of the yearly scenarios, as well as the linkage to the four phases, PREVENT, DETECT, MITIGATE and REACT is also considered in the table. With the design of this table, it is possible to select requested activities like “all projects with relevance to DETECT phase” or “all projects with relevance to the scenario of the year 1” with just a few clicks.

Other important data, such as e.g. classification of the projects, can be found in the column “Comments”. The key element “Developed Tools: Categories” gives basic information on the kind of tool which is/have been developed during the project, mainly technology or knowledge. An excerpt of the research activity list can be found in Annex 1 (see at page **Fel! Bokmärket är inte definierat.** in this document).

More than 170 projects have now been listed in the table and as much information as possible have been added. Many EXERTER partners participate, or have participated, in several of the listed projects and have therefore been able to provide information about them. The Excel table includes only unclassified information and will be extended continually. Through communication and interaction with other projects (e.g. ERNCIP), as well as web searches and special workshops or conferences, additional research activities will be identified and included in the research activity list.

3.3 Review of research activities in the different counter attack domains

From the generic overview a selection of the most auspicious research activities, which can counter existing practitioner needs and gaps in the field of SoE relating to the defined scenario and its key aspects highlighted in deliverable D6.1 Annex 1, is further studied. The research projects have been divided into the four counter attack domains, prevent, detect, mitigate and react, based on their research.

With the scenario of the 1st year (Oslo bombing) in mind a preliminary selection of projects has been divided into the four counter attack domains, presented below. The selection might be modified later on. Some research initiatives that previously were pointed out as interesting and recommended as relevant to include in the the annual workshop, (see EXERTER milestone 1) were BONAS, EMPHASIS, STYX, SHIELD, ENTRAP and EXPEDIA.

3.3.1 Prevent

For the prevent domain the following projects were selected:

- BONAS (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 (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.
- ERNCIP (European Reference Network for Critical Infrastructure Protection): ERNCIP aims at providing a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonise test protocols throughout Europe.
- EXPEDIA (EXplosives Precursor Defeat by Inhibitor Additives): EXPEDIA dealt with research in the area of the supply chain of explosive precursors, the illegal production of initiator systems (primary explosives), chemical inhibition of explosive precursors (main charges) and early detection of bomb factories. It has created a European guide for first responders in form of an application for smartphones.
- LOTUS (LOcalisation of Threat substances in Urban Society): LOTUS aimed to create a demonstration system by which illicit production of explosives and drugs can be detected during the preparation and production phase of a terrorist plot.
- PREVAIL (PRecursors of ExplosiVes: Additives to Inhibit their use including Liquids): PREVAIL dealt with the restriction to get at precursor chemicals to synthesise HMEs and to develop a series of novel inhibitors of explosives production from some common starting ingredients as well as markers to enable fertiliser-based explosives detection.

3.3.2 Detect

For the detect domain the following projects were selected:

- C-BORD (effective Container inspection at BORDer control prints): The aim of C-BORD was to develop and test a cost-effective prototype (in action) for the generalised inspection of container and large-volume freight in order to protect EU borders, coping with a large range of container non-intrusive inspection (NII) targets, including explosives.
- EFFISEC (EFFicient Integrated SEcurity Checkpoints): EFFISEC dealt with the security at checkpoints (land and maritime) and aims to deliver more efficient technological equipment to border authorities.
- EUROSKY (Single European Secure Air-cargo Space): EUROSKY aimed to deliver a high impact programme for advanced air-cargo security and facilitation measures to safeguard international supply chains and the security of citizens while fostering international co-operation and a broad stakeholder engagement from all segments of the air-cargo industry.
- IMSK (Integrated Mobile Security Kit): The aim of IMSK was to combine technologies for area surveillance, checkpoint control, CBRNE detection and support for VIP protection into a mobile system for rapid deployment at venues and sites which temporarily need enhanced security.

- EDEN (End-user driven demo for CBRNE): The EDEN project aimed to leverage the added-value of tools and systems from previous R&D efforts and improve CBRNE resilience through their adaptation and integration in complex multi-national/agency CBRNE operations.

3.3.3 Mitigate

For the mitigate domain the following projects were selected:

- ELASSTIC (Enhanced Large Scale Architecture with Safety and Security Technologies and special Information Capabilities): ELASSTIC contained the topics building design concepts and sensor technologies and dealt with the safety, security and resilience of building complexes towards natural and man-made disasters.
- SPIRIT (Safety and Protection of built Infrastructure to Resist Integral Threats): SPIRIT developed tools to reduce damage destruction and disruption to large new and existing buildings to enhance the security of large buildings against terrorist CBRE threats.
- VITRUV (Vulnerability Identification Tools for Resilience Enhancements of Urban Environments): VITRUV considered urban planning, vulnerability assessment and resilience enhancement for designing secure cities.
- ENCOUNTER (Explosive Neutralisation and Mitigation Countermeasures for IEDs in Urban/Civil Environment): ENCOUNTER aimed to develop methods and technologies needed to identify, explore and validate innovative techniques for mitigation and neutralization of (VB)IEDs, also blast/fragment impact mitigation methods, in urban/civil environment.
- TACTICS (Tactical Approach to Countering Terrorists in Cities): TACTICS aimed to identify, research and develop tools, technologies and methods to improve the effectiveness of security forces in preventing and dealing with an urban attack. Therefore, topics as CCTV and threat management were considered.
- AVERT (The Autonomous Vehicle Emergency Recovery Tool): The aim of AVERT was to provide a unique capability to Police and Armed Services to rapidly deploy, extract and remove both blocking and suspect vehicles from vulnerable positions such as enclosed infrastructure spaces, tunnels, low bridges as well as under-building and underground car parks.
- EDEN (End-user driven demo for CBRNE): The EDEN project aimed to leverage the added-value of tools and systems from previous R&D efforts and improve CBRNE resilience through their adaptation and integration in complex multi-national/agency CBRNE operations.
- SUBCOP (Suicide Bomber Counteraction and Prevention): Within SUBCOP technologies and procedures have been developed that can be applied by the Police Security Forces when responding to a suspected PBIED (Person Borne Improvised Explosive Device) in order to isolate the attacker using a ballistic, fast inflatable structure to minimise the effects of an explosion with bomb fragments.

3.3.4 React

For the react domain the following projects were selected:

- ACRIMAS (Aftermath Crisis Management System-of-systems Demonstration – Phase I): ACRIMAS dealt with the assessment of Europe's general CM performance especially in terms of weaknesses and gaps. The aim was to prepare a Demonstration Programme on Aftermath Crisis Management by delivering a strategic roadmap and also a demonstration concept for Phase II.
- BRIDGE (Bridging Resources and Agencies in large-scale Emergency Management): The goal of BRIDGE was to build a system supporting interoperability to improve crisis and emergency management in the EU Member States.

- E-SPONDER (Holistic approach towards the first responder of the future): E-SPONDER aimed to develop and demonstrate a prototype management system which provides actionable information and communication support to first responders (between forces on the ground (police, rescue, firefighters) and out-of-theatre command and control centres (CC)) that act during abnormal events (crises).

- SAVASA (Standards based Approach to Video Archive Search and Analysis): The objective of SAVASA was to create a video archive search platform that allows authorised users performing semantic queries over various remote and non-interoperable video archives. This project has exploited the current trends in computer vision, video retrieval and semantic video analysis.

- FORLAB (Forensic Laboratory for in-situ evidence analysis in a post blast scenario): FORLAB aimed to provide a novel systematic methodology for optimizing forensic evidence collection by developing a system of highly advanced analytical forensic technologies (LIBS-RAMAN, LIF, NLJD) for sample screening and 3D scenario recreation in just a few minutes.

- HYPERION (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.

- ROSFEN (Rapid On-Site Forensic analysis of Explosives and Narcotics): The goal of ROSFEN was to deliver a compact system for rapid, on-site direct detection and lab-quality analysis of explosives and their precursors. A prototype system, based on a miniaturised solid state quadruple mass-spectrometer detector, can detect explosives with sensitivity and selectively comparable to state of the art laboratory instrument.

- SUSQRA (Schutz vor unkonventionellen Sprengvorrichtungen – Charakterisierung und quantitative Risikoanalyse, English transl.: Protection against improvised explosive devices (IEDs) – characterization and quantitative risk analysis): The aim of SUSQRA was to develop a software which can determine the extent of damage inflicted by IEDs, also for the forensic post blast and fragment dispersion evaluation.

4 Standardisation and certification priorities

4.1 Introduction

Work related to standardisation and certification in relation to the yearly scenario and its key elements (highlighted in D6.1 Annex 1, and in Annex 4 to this report) is presented in the following section. Standardisation, certification and regulation affects the possibilities for innovations to reach the market and it can contribute to filling the identified capability gaps, see Section 2 and Annex 4 to this report.

Work related to standardization and certification is under progress. Through interactions with practitioners, private sector and standardization bodies an assessment of relevant standards, CEN (European Committee for Standardization), CENELEC (European Committee for Electrotechnical Standardization) & ISO (International Organization for Standardization), IEC TC (International Electrotechnical Commission Technical committees) and other working groups (WG) relevant for the EXERTER project has been performed, see Section 4.2. By reaching out to certification entities and to possible relevant projects, contacts and collaborations are being set up. Extending the work to cover certification and regulation initiatives is the next step, and action to communicate the opportunities on standardisation, certification and regulation to the relevant entity will be continued in the coming work.

4.2 Overview of standardisation and certification initiatives

The technical comities (TC) and standardisation initiatives that are currently deemed relevant for EXERTER have been assessed, and a selection of them is listed below for the respective counter-attack domains. The standardisation entities have also been contacted to create a foundation for future collaboration.

Standardisation entities of particular interest are for example CEN/TC 391 Societal and Citizen Security and ISO/TC 292 Security and resilience. Linked to the current scenario (Oslo, 2011), specifically CEN/TC 160 Fertilizers and liming materials can be mentioned due to its connection with the materials used to create the bomb.

4.2.1 Prevent

A subset of the standardisation initiatives that have been identified as relevant for the prevent domain in general are listed in Table 1. A full table is given in Annex 2.

Table 1. Standardisation entities relevant for the counter-attack domain Prevent

Entity	TC/WG	Energetic materials for defence - Safety, vulnerability - Friability	Description
CEN	TC 212	Pyrotechnic articles	Standardization of fireworks, theatrical pyrotechnic articles, pyrotechnic articles for vehicles and other pyrotechnic articles, particularly from the point of view of their safe use.
CEN	TC 160	Fertilizers and liming materials	Harmonization of denominations, specifications, marking, methods of test (physical and/or chemical) and safety conditions, related to fertilizers and Liming materials. Work on items covered by EEC directives currently existing should only be undertaken at the invitation of the Commission.
CEN	TC 305	Potentially explosive atmospheres - Explosion	To develop standards where necessary in the fields of: - test methods for determining the flammability characteristics (ignition, propagation, explosion effects, etc.) of substances; - equipment and protective systems for use in potentially explosive

		prevention and protection	atmospheres and equipment and systems for explosion prevention and protection.
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 264	Fireworks	Standardization in the field of Fireworks, including quality control, definitions, terminology, classification, categorization, labelling, test methods and basic safety requirements.
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.

Other initiatives related to regulation, guidelines and standardisation

The EU regulation on the marketing and use of explosives precursors, EU Regulation 98/2013, is central for the prevention domain. It regulates the availability and allowance to possess certain chemicals, e.g. ammonium nitrate, for the general public. An update of the regulation is underway.

4.2.2 Detect

Standardisation initiatives

A selection of standardisation initiatives and technical comities related the detection domain are listed in Table 2 below. The full list is provided in Annex 2. There are also some standardisation initiatives that concern materials that could be of interest to the detect domain, e.g. ISO/TC 264 Fireworks, CEN/TC 321 Explosives for civil uses, CEN/TC 160 Fertilizers and liming materials and CEN/TC 212 Pyrotechnic articles. These have been excluded here but are presented in Table 1 (Prevent).

Table 2. Standardisation entities relevant for the counter-attack domain Detect

Entity	TC/WG	Energetic materials for defence - Safety, vulnerability - Friability	Description
CEN	TC 264	Air quality	Standardization of methods for air quality characterization of emissions, ambient air, indoor air, gases in and from the ground and deposition, in particular measurement methods for air pollutants (for example particles, gases, odours, microorganisms) and methods for the determination of the efficiency of gas cleaning systems. Excluded are: - the determination of limit values for air pollutants; - workplaces and clean rooms; - radioactive substances.
CEN	TC 388	Perimeter Protection	Standardisation in the field of perimeter protection including systems and products (as part of the system) from the security perspective point of view, without neglecting safety aspects
CEN	TC 391	Societal and Citizen Security	See Prevent
ISO	TC 158	Analysis of gases	Standardization in the field of analysis of gases, including: terminology, preparation of gas mixtures, sampling, and transfer lines; analytical methods including evaluation of characteristics of the analysers. Excluded: subjects falling within the scope of any other ISO technical committee (e.g. ISO / TC 28, ISO / TC 146 and ISO / TC 193) unless specifically requested.
ISO	TC 161	Controls and protective devices for gas and/or oil	
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.

Other initiatives related to regulation, guidelines and standardisation

Existing standards and guidelines related to the detection domain is for example treated in the ERNCIP report Detection of Explosives and Weapons in Secure Locations (DEWSL) - Final Report Phase 1, JRC, 2016. In the context of this year's yearly scenario in EXERTER it can be concluded that existing guidelines and standards are focused on the aviation security and customs areas for detection of explosives. It could also be noted that some procedures for vehicle screening exist.

In the aviation security area there are standards related to equipment performance and testing, but it is noted that these performance standards and test methods may be too stringent for vehicle screening at secure locations. Other standards (e.g. ASTM) are seen to likely be possible to apply to vehicle screening.

According to the DEWSL report[3] there are no known dedicated general processes, methods, equipment standards or guidelines in the EU for screening vehicles for the presence of explosives and weapons with the aim of protecting civil secured facilities.

However, there are different operations where general vehicle screening is performed, e.g. in aviation security, by customs authorities, by the police and by military forces. In aviation security there is a legally binding international guideline, AVSEC (EC185 /DEC774), where two methods for vehicle (other than cargo) screening are described. One is hand search with indication of areas of special attention and the second is visual search. For cargo screening detailed rules exist, as well as equipment performance standards. For customs authorities, screening procedures aims at detecting a range of goods and materials such as drugs, precursors, explosive devices and weapons. The European Commission DG-TAXUD encourages harmonized approaches through dissemination of knowledge, guidance, and best practice. In the military, vehicle screening operations for the detection of hidden bombs (IEDs) and firearms are widely applied. According to the DEWSL report [4], EDA (European Defence Agency) does not own standards in this area, although they do engage in concept development for protection of critical infrastructure. NATO (North Atlantic Treaty Organization) has developed TTPs (Tactics, Techniques and Procedures) and doctrines to support various staff levels in the search of vehicles, including for VBIEDs. The police screens vehicles for detection of hidden criminal goods including weapons. It may be assumed that guidelines exist at national levels.

[3] Detection of Explosives and Weapons in Secure Locations (DEWSL) - Final Report Phase 1, JRC, 2016

[4] Detection of Explosives and Weapons in Secure Locations (DEWSL) - Final Report Phase 1, JRC, 2016

4.2.3 Mitigate

Standardisation initiatives

Table 3. Standardisation entities relevant for the counter-attack domain Mitigate

Entity	**TC/WG**	**Energetic materials for defence - Safety, vulnerability - Friability**	**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 388	Perimeter Protection	Standardisation in the field of perimeter protection including systems and products (as part of the system) from the security perspective point of view, without neglecting safety aspects
CEN	TC 72	Fire detection and fire alarm systems	To prepare standards, harmonised where necessary to meet the essential requirement 'Safety in case of fire' of the Construction Products Directive, in the field of fire detection and fire alarm systems in and around buildings, covering test methods, requirements and recommendations for: - components; - the combination of components into systems; - the planning, design and installation of systems for use in and around buildings; - usage, maintenance and servicing; - the connections to and control of other fire protection systems; - the combination with other systems to form integrated systems; - the combination with fixed firefighting systems; - the contribution of fire detection and fire alarm systems to fire safety engineering.
CEN	TC 391	Societal and Citizen Security	See Prevent
ISO	TC 92	Fire safety	Standardization of the methods of assessing fire hazards and fire risk to life and to property, the contribution of design, materials, building materials, products and components to fire safety and methods of mitigating the fire hazards and fire risks

			by determining the performance and behaviour of these materials, products and components, as well as of buildings and structures. Excluded: materials and equipments already covered by other technical committees; fields covered by other ISO and IEC committees.
ISO	TC 185	Safety devices for protection against excessive pressure	Standardization in the field of safety devices for protection against excessive internal and external pressure. Excluded: valves predominantly made of plastics which are the responsibility of ISO / TC 138; components intended for use primarily in fluid power systems which are the responsibility of ISO / TC 131.
ISO	TC 292	Security and resilience	See Prevent
CLC	TC 31	Electrical apparatus for potentially explosive atmospheres	To standardize the general requirements for the construction and testing of electrical apparatus for potentially explosive atmospheres and the specific requirements for the construction and testing of electrical apparatus. Type of protection "o" (oil immersed) and type of protection "q" (powder filled) and types with protection for use in the presence of combustible dusts, and to co-ordinate the work of the sub-committees dealing with the standardization of specific requirements for other individual types of protection.

Other initiatives related to regulation, guidelines and standardisation

The manual "Reference Manual to Mitigate Potential Terrorist Attacks against Buildings FEMA-426/BIPS-06/October 2011" is a part of the new Building Infrastructure Protection Series published by the United States (U.S.) Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Infrastructure Protection and Disaster Management Division (IDD). It serves to advance high performance and integrated design for buildings and infrastructure. This manual was prepared as a component of a program related to infrastructure protection and disaster management; the overall goal of this program is to enhance the blast and chemical, biological, and radiological (CBR) resistance of buildings and infrastructure to meet specific performance requirements at the highest possible level.

4.2.4 React

Standardisation initiatives

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

Entity	**TC/WG**	**Energetic materials for defence - Safety, vulnerability - Friability**	**Description**
CEN	TC 162	Protective clothing including hand and arm protection and lifejackets	To prepare European Standards (requirements and testing) in the field of clothing to protect against physical and chemical hazards.

CEN	TC 192	Fire and Rescue Service Equipment	Standardization of equipment and vehicles for rescue and firefighting. Personal protective equipment covered by CEN/TC 191 is excluded.
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 305	Potentially explosive atmospheres - Explosion prevention and protection	To develop standards where necessary in the fields of: - test methods for determining the flammability characteristics (ignition, propagation, explosion effects, etc.) of substances; - equipment and protective systems for use in potentially explosive atmospheres and equipment and systems for explosion prevention and protection.
CEN	TC 391	Societal and Citizen Security	See Prevent
CEN	TC 72	Fire detection and fire alarm systems	See Mitigate
CEN	TC 85	Eye protective equipment	Establishment of specifications and test methods relevant to eye and face protectors.
ISO	TC 21	Equipment for fire protection and fire fighting	Standardization in the field of all fire protection and firefighting apparatus and equipment including extinguishing media as well as the personal equipment of the fire fighter, and related work on terminology, classification and symbols. Approval of advisory documents relating to the general principles and application of equipment and apparatus for fire protection and firefighting.
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	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.

5 Exploitation support

5.1 Introduction and overview

Technology and tools are central in countering the terror threat and bridging the gaps and requirements identified in D6.1 Annex 1 and in Annex 4 to this report. 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.

To get an overview of the market and technologies, information from other projects have been used as a starting point. Two EU projects where technological assessments have been performed are:

1. The FP7-project HECTOS, which focussed on the harmonization of evaluation, certification and testing of physical security products, and
2. The JRC-project ERNCIP (European Reference Network for Critical Infrastructure Protection), which aims at providing a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonise test protocols throughout Europe.

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).

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

The overview of physical security products provided by HECTOS have been used to choose different categories of technologies, which can help in the fight against terrorist attacks. A first draft from the generic overview of the state-of-the-art technologies has been compiled in a simple Excel table.

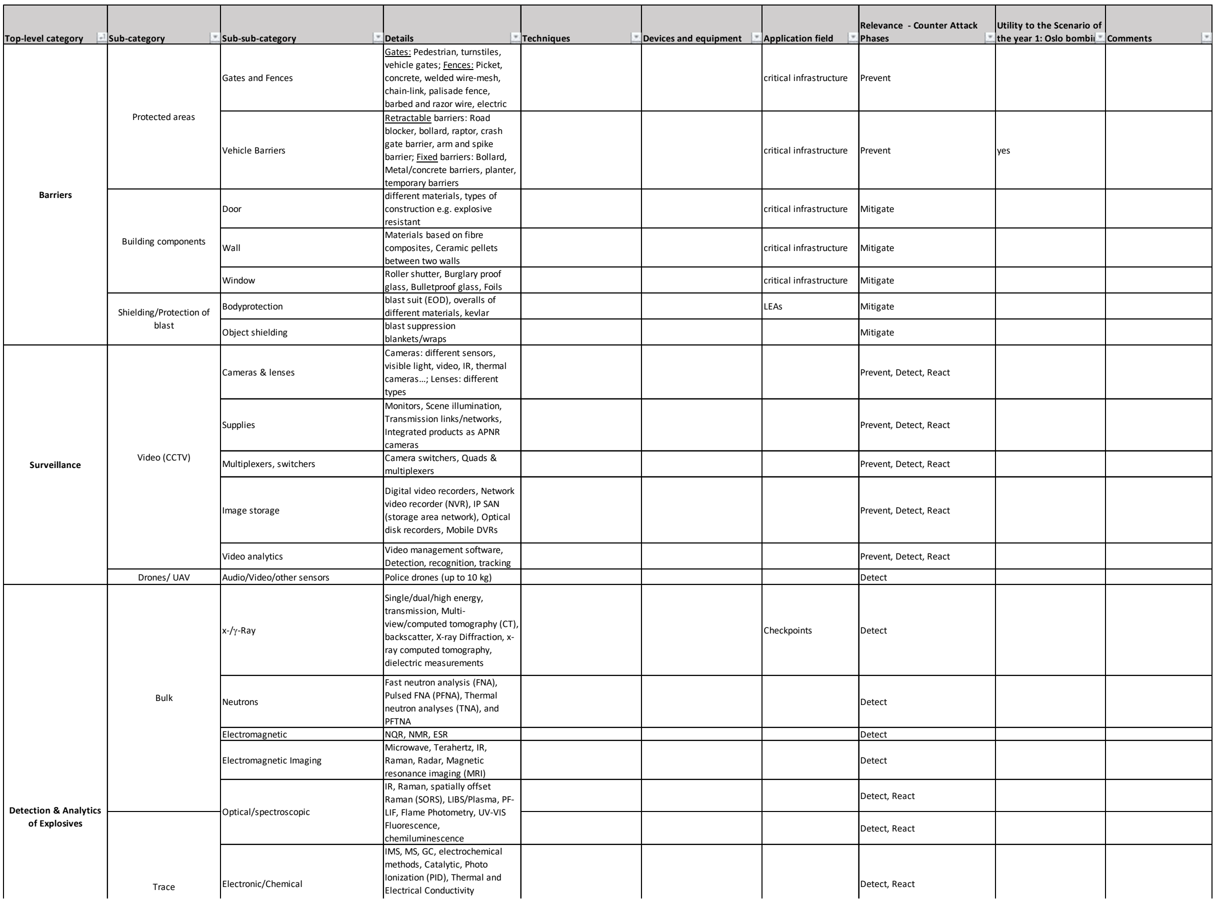
For the sake of clarity it is not possible to include too many details of the technologies in the Excel table. Important key elements have been defined as, e.g.:

- Top-level category,
- Sub-category,
- Application field,
- Relevance - Counter Attack Phases and Relevance to the Scenario of the year 1: Oslo bombing

The “Top-level categories” included to date are: Barriers, Surveillance, Detection & Analytics of Explosives, Other Detection, and Security/Crisis Management.

The key elements and the content of the table are not predetermined up to the present date, but the concept is established. Developing the table and its structure is still work in progress and it will be further elaborated on within the consortium. The table below, Table 5, is a first draft that will be expanded and improved. The full table (still first draft) is included in Annex 3.

Table 5. A draft of the generic overview of technologies



Top-level category	Sub-category	Sub-sub-category	Details	Techniques	Devices and equipment	Application field	Relevance - Counter Attack Phases	Utility to the Scenario of the year 1: Oslo bombi	Comments
Barriers	Protected areas	Gates and Fences	Gates: Pedestrian, turnstiles, vehicle gates; Fences: Picket, concrete, welded wire-mesh, chain-link, palisade fence, barbed and razor wire, electric			critical infrastructure	Prevent		
		Vehicle Barriers	Retractable barriers: Road blocker, bollard, raptor, crash gate barrier, arm and spike barrier; Fixed barriers: Bollard, Metal/concrete barriers, planter, temporary barriers			critical infrastructure	Prevent	yes	
	Building components	Door	different materials, types of construction e.g. explosive resistant			critical infrastructure	Mitigate		
		Wall	Materials based on fibre composites, Ceramic pellets between two walls			critical infrastructure	Mitigate		
		Window	Roller shutter, Burglary proof glass, Bulletproof glass, Foils			critical infrastructure	Mitigate		
	Shielding/Protection of blast	Bodyprotection	blast suit (EOD), overalls of different materials, kevlar			LEAs	Mitigate		
		Object shielding	blast suppression blankets/wraps				Mitigate		
Surveillance	Video (CCTV)	Cameras & lenses	Cameras: different sensors, visible light, video, IR, thermal cameras…; Lenses: different types				Prevent, Detect, React		
		Supplies	Monitors, Scene illumination, Transmission links/networks, Integrated products as APNR cameras				Prevent, Detect, React		
		Multiplexers, switchers	Camera switchers, Quads & multiplexers				Prevent, Detect, React		
		Image storage	Digital video recorders, Network video recorder (NVR), IP SAN (storage area network), Optical disk recorders, Mobile DVRs				Prevent, Detect, React		
		Video analytics	Video management software, Detection, recognition, tracking				Prevent, Detect, React		
	Drones/ UAV	Audio/Video/other sensors	Police drones (up to 10 kg)				Detect		
Detection & Analytics of Explosives	Bulk	x-/γ-Ray	Single/dual/high energy, transmission, Multi-view/computed tomography (CT), backscatter, X-ray Diffraction, x-ray computed tomography, dielectric measurements			Checkpoints	Detect		
		Neutrons	Fast neutron analysis (FNA), Pulsed FNA (PFNA), Thermal neutron analyses (TNA), and PFTNA				Detect		
		Electromagnetic	NQR, NMR, ESR				Detect		
		Electromagnetic Imaging	Microwave, Terahertz, IR, Raman, Radar, Magnetic resonance imaging (MRI)				Detect		
		Optical/spectroscopic	IR, Raman, spatially offset Raman (SORS), LIBS/Plasma, PF-LIF, Flame Photometry, UV-VIS Fluorescence, chemiluminescence				Detect, React		
	Trace						Detect, React		
		Electronic/Chemical	IMS, MS, GC, electrochemical methods, Catalytic, Photo Ionization (PID), Thermal and Electrical Conductivity				Detect, React		

5.3 Support for collaboration and exploitation

In the End user and Expert Community (EEC) in EXERTER there are only a few Industries and SME:s (I) at project start, compared to the rest of the pillars (RTO, End user (E_U) and Academia (A)). In order to extend the network it is necessary to screen the European industrial market to find companies that could be useful and add value to the EXERTER project, and to then evaluate the possibility to include them in the EEC or to engage with them in other ways, e.g. consultations or other networking activities. The main purpose is to cover a wide range of counter tool technologies, avoiding overlaps between them in different fields of knowledge.

By engaging the EXERTER EEC and others in the network at the EXERTER workshop, the project can collect information about how to bridge the gaps among I-RTO-E_U-A. Using different techniques, such as questionnaires, validating methodologies (e.g. Dual uses for developed technologies in different fields or new applications for avant-garde inventions) or protocols to transfer knowledge between I-RTO-E_U-A would be the key to improved collaboration and exploitation possibilities.

The actions and plans taken so far have been based on a SWOT analysis (or SWOT matrix). This analysis is a strategic planning technique used to identify strengths, weaknesses, opportunities, and threats related to the project EXERTER, in terms of exploitation. The name is an acronym for the four parameters the technique examines in this project:

Strengths: characteristics that give EXERTER an advantage over other projects.

- The creation of European programs such as the EXERTER.
  - An adequate technological and security defence industrial base can-not be sustained exclusively from the national point of view, which will have to enhance its projection

at European level and thus obtain a networking capacity beyond the sum of each of the national parts.

Weaknesses: characteristics of the project that place it at a disadvantage relative to others.

- Many of the requirements and needs identified for the four counter attack domains (prevent, detect, mitigate and react), are classified as EU-Restricted.
    - This characteristic usually means that the scientific and technological requirements are not presented to, or can be difficult to discuss with, industry until at later stages.
    - In addition, the research and tests following the needs and requirements is often also classified, which might hinder the transfer of knowledge resulting from research and development.

Opportunities: elements in the environment that the project could exploit to its advantage.

- Until now, there is a lack of involvement of specialized companies in the four counter attack domains in EXERTER. For this reason, EXERTER will work on increasing contacts with companies involved in the development of technology in each of the four domains.
- It is possible that already existing technologies can be used in an innovative way to bridge the identified gaps, and that no new technology or deep research will be needed.

Threats: elements in the environment that could cause trouble for the project.

- The actors involved must have a rapid capacity to react to the evolution of the techniques and countermeasures of the threat that are revealed in the explosive devices as well as in their use.

6 Analysis and recommendations

6.1 Overview

This section contains analyses and recommendations in the domains prevent, detect, mitigate and react. The analyses are based on the gaps and requirements identified for this year's scenario (described in Annex 4 to this report, and a shortlist is given in D6.1 Annex 1) and the information described in sections 3 to 5 in this report on research initiatives, state-of-the-art technologies and exploitation and standards and certification, see Figure 2.

The analysis for the prevent domain is given in a EU confidential annex, D6.2 Annex 5. Information regarding the other domains are presented in sections 6.3 to 6.5 below.

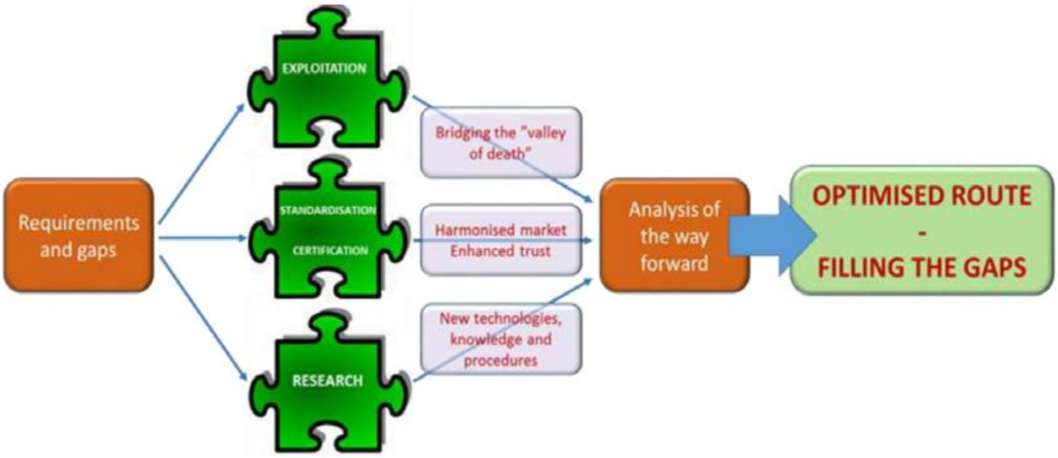


Figure 2. A schematic image describing the flow of information used in EXERTER to fill identified gaps, identify other gaps, and making progress in the project.

6.2 Prevent

Information is provided in an annex classified EU confidential, Annex 5.

6.3 Detect

In the context of this year's scenario, the 22nd July 2011 Oslo bombing, the detect domain is mainly focused around detection of VBIEDs and ammonium nitrate based HMEs in a short timeframe.

The problem of VBIED detection can be split into two main operational categories:

- checkpoint screening in both fixed and portable checkpoint configurations for trace and bulk detection
- mobile or portable applications to determine from a distance whether or not a suspicious vehicle is a VBIED.

For vehicle screening, there is a lack of suitable detection equipment. There is a need for research into new detection technologies and novel ways of using existing technologies and combinations of technologies, perhaps from other fields. There are a number of tools that could be applied for vehicle screening at a checkpoint location. Some of these already exist and simply require promotion and dissemination, others do not exist or require further development. The way a suspicious vehicle could be identified is by e.g.:

- Driver Identification with Facial Recognition
- Solid trace detection
- Vapour trace detection
- Bulk explosives detection
- Device component detection

- License Plate Security Cameras

At European level, there are several research initiatives where the developed tools could potentially be applied for vehicle screening. Some European projects that are partially applicable to the Oslo are the projects C-BOARD, EFFISEC and IMSK. C-BORD worked with generalised inspection of container and large-volume freight. The applied techniques were Advanced Radiation Management, Next Generation Cargo X-Ray, Tagged Neutron Inspection, Photofission and Evaporation Based Detection. EFFISEC focused on integrated security checkpoints. The project aimed at developing technology for automatic gates, portable identity check and scanning equipment to be used for in depth controls of travellers, luggage and vehicles, for pedestrians and people inside vehicles. The last selected project, IMSK, focused on mobile solutions, and covered technologies for area surveillance, security checkpoints, CBRNE detection and support for VIP protection. The system was to allow rapid deployment at venues and sites (hotels, sport/festival arenas, etc) which temporarily need enhanced security. Employed technology was various new sensors for threat detection and validation, including cameras (visual & infrared), radar, acoustic and vibration, x-ray and gamma radiation and CBRNE.

In general, new technologies for explosives detection need to be able to identify a broad range of materials with low false alarm rates and the ability to rapidly detect threats or anomalies from a complex vector such as a vehicle.

Screening processes could include stand-off detection of trace contamination, vapour detection technologies and techniques for detecting concealed explosives whilst the driver and passengers are still in the vehicle. Some requirements on technology for vehicle screening are for example:

- Easy to use, with minimal operator training to allow efficient screening
- Applicable to any of the types of vehicles likely to be encountered where the detection system is deployed
- Able to quickly adjust screening capabilities to accommodate any size vehicle
- Able to screen as much of the vehicle's exterior as possible or specific areas can be predetermined for screening ("Hot spots", such as door handles and other primary contact points);
- Able to identify the location of the explosives within the vehicle

Some of the gaps that have been identified are the following:

- Training for:
    - CCTV operatives and security staff. (suspicious behaviour related to IED attacks, attendance to tailored conferences given by EOD Teams;
    - first responders (police, fire fighters, ambulance) to identify and notice the presence of potential secondary devices.
- Automatic license plate and vehicle security cameras:
    - database system for automatic identification of vehicles (ability to alert if a vehicle is not frequent in the target location);
    - automatic alert in case of presence of one unauthorized vehicle;
    - database with the frequent vehicles authorized to enter in sensitive areas;
    - information shared with LEA officers;
    - information about illegal parking shared with LEA officers.
- New methods to identify suspicious behaviours (people, vehicles):
    - new ways of raising citizens' awareness;
    - develop automatic systems for controlling and reporting.
- Driver Identification with Facial Recognition with CCTV system:
    - database of names (suspicious people, vehicles);
    - quick information shared with LEA officers.
- Stand-off detectors (traces, bulk, anomalies, non-chemical components, etc.) (e.g. for unusual chemical signals/off-gassing).

Training courses and guidelines for vehicle screening operations are also lacking.

6.4 Mitigate

Several research initiatives already addressed aspects related to possible mitigation measures that could be implemented in a scenario directed at a government facility within an urban and publicly accessible environment. Some exemplary projects addressing key aspects are subsequently described. While these projects resulted in physical technical solutions, the key to become effective mitigation measures lies in the implementation and use of the respective technical solutions. Standardization, certification and improved availability of technical solutions can help mitigate the effects of future attacks.

Regarding the particularities of the defined scenario, a number of past research initiatives address aspects improving the mitigation of explosion effects (Section 3.3.3). For example, SPIRIT and ELASSTIC aimed at improving the physical security of large buildings, specifically in an urban environment. The focus of ENCOUNTER was on the neutralization of IEDs and connected explosion effect mitigation during the neutralization process. SUBCOP had proposed a shield type configuration to isolate suicide bombers in order to minimise the effects of an explosion. AVERT, added another point of view by describing methodologies to remove the potential threat source from the scene. Exemplary projects researching on organizational measures were TACTIS or EDEN, which aimed at improving the effectiveness of security forces and at enabling them in a proper situational assessment.

It can be observed from the first project-year scenario that potential solutions to mitigate explosion effects existed. Barriers or bollards surrounding the building to be protected and an appropriate landscape design can increase stand-off zones as one of the most important mitigation measure to reduce blast effects. The implementation of stand-off zones has to be combined with an appropriate access control (blast proof designed), which furthermore would allow to install instruments in order to scan entering vehicles (or people) for explosive traces, license plate cross-checks or to identify suspicious behaviours and perform face recognitions. Finally, organisational measures, as emergency- and evacuation plans or even the neutralization of the (VB)IED can mitigate the effects from the explosion.

In conclusion, related to measures aimed at mitigating explosion effects to protect the exposed populace, reaction forces and the built environment, several physical security technologies are already available, but can certainly be investigated further to widen the spectrum of potential possibilities to react to threats similar to the defined first project-year scenario. Possibilities for future research include:

- Research aimed at the development of mobile structural components to reduce explosion effects
- The development of organizational procedures once a threat is detected
- While single component IEDs are easily characterized, the assessment of the specifics of a VBIED threat up to the same quality level available for small and simplistic explosive sources is still an open research opportunity
- How to integrate physical security assessment and respective planning into the common design process?
- How to make existing solutions more readily available to the end user community?
- Basic research on physical security aspects (protection, potential hazards) of “new” façade components and load-bearing components and their integration within a building structure. For example:
    - Large glazing systems
    - Photovoltaic façade systems
    - Timber panels
    - Load-bearing columns
    - New materials: Carbon-free concrete, mycelia-reinforced concrete etc.

Moreover, future research is necessary on how to introduce the research results more widely to the end user community and on how to make the implementation of research results more common practice.

With respect to mitigate the explosion effects using physical security measures, during future designs of new-, or the retrofit of existing buildings, some major challenges have to be addressed. Urban buildings in major European cities, as the governmental building in Oslo, still have to remain their functionality, must be affordable and should be open and inviting with good urban qualities (it cannot be aimed to build a shelter). The design philosophy should furthermore be, not to cause additional injuries by the structure, e.g. originated from the glazing, ceiling or progressive building collapse. In order to balance out the security/protection level with other targets (as costs, architectural parameters, environment, and office spaces), structural vulnerability assessments as well as an iterative risk management approach is strongly recommended.

Consequently, initiatives aimed at developing procedural standards (e.g. quantitative risk analysis in the design process of critical infrastructure), design guidelines and certification of protection standards are needed.

In terms of exploiting research results, there is a need to put more emphasis on transferring the knowledge gained within the research projects to potential end users. This includes making results more accessible technically, but also on a "language level" that enables end users to directly transfer research results into their respective field of application.

6.5 React

Due to large differences regarding national and local frameworks, procedures and the structure of law enforcements agencies and emergency services, international standardisation with respect to the post-blast work is challenging. Certifications target the reduction of risks, when handling of hazardous chemicals is to be expected. These may include guidelines and requirements for warning systems and personal protective equipment for instance.

Since different national regulations and responsibilities come into effect among different countries, applicable standardisation which comes into place in the aftermath of an extensive emergency is scarce. Nevertheless, several research projects deal with the topic of crisis management. It is unclear to what extend these research efforts can be or are being transferred into standard operating procedures and the practical work.

A considerable amount of research appears to be conducted in the area of standoff detection of hazardous substances and in the field forensic analysis. The implementation of these techniques into best practice manuals or standardised procedures cannot be observed, possibly due to the lack of commercially available systems.

7 Future work

A preliminary selection of projects that are of special interest for EXERTER have been finalised, and approximately five to eight projects have been selected for each counter attack domain. These projects and research activities have been examined in more detail, and studied in relation to the identified gaps and needs. This work will be continued within EXERTER throughout the project with different focus areas. Information on research activities which can play a role in the identified gaps will be further lifted for discussion, and considered as topics for the next annual workshop.

Regarding standardisation and certification, the efforts until now have mainly been focused on identifying standardisation entities related to EXERTER in general, and to establish connections with these entities. Some identified standardisations, e.g. related to security and resilience, are directly relevant for the current scenario, and others are more indirectly coupled to counter-tools and/or a terror attack in the different counter attack domains. Central for the future work is to extend the review to better cover certification and regulations. It is in addition important to further identify and analyse gaps in current standardisations and certifications in relation to the yearly scenario, and to find opportunities for bridging these gaps.

An initial inventory of technologies that could prevent, detect, mitigate and/or react to a terror attack have been set up. It is important to highlight the technologies with particular relevance to the yearly scenario, and to link them to the terrorist timeline. This will be implemented by selecting products from the generic overview of technologies, these will then be studied in detail and summarized in separate reports. Taking into account the current knowledge and experience, it is also planned to include more companies dedicated to each of the counter attack domains in EXERTER and to study different types of technologies that are currently developed (not for anti-terrorism purposes) which might have the possibility to be used within the counter attack domains.

Work on identifying methods to facilitate the transfer of knowledge from universities to companies will be continued, and consultations will be set up.

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