22/05/2023

Version no. 1.0

D6.10
EXERTER 10th report on innovations, standardisation and exploitation within SoE

FOI
KEMEA
TNO
BKA
PSNI
FhG-ICT
FhG-EMI
INTA

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

PUBLIC

D6.10
EXERTER 10th report on innovations, standardisation and exploitation within SoE

Main Author(s) - (Public)	
Name	*Organisation*
Bernhard Zachhuber	FOI
Anneli Ehlerding	FOI
Emma Lundell	FOI
Michael Wittek	FhG-ICT
Oscar van der Jagt	TNO
Maria Ángeles Contreras Jaén	INTA
Rasmus Schulte-Ladbeck	BKA
Jonathan Middleton	PSNI
Ioannis Daniilidis	KEMEA
Contributors	
Johannes Schneider	FhG-EMI
Juan José Navlet Salvatierra	INTA
Georgios Antonopoulos	KEMEA
Frank Schnürer	FhG-ICT
Juan José Navlet Salvatierra	INTA
Malte von Ramin	FhG-EMI
Roberto Chirico	ENEA
Tina Fröhlich	BKA

Document information	
Version no.	*Date*
0.1	2023-05-16
1.0	2023-05-22

Summary

This document is the tenth of the 6-monthly Deliverables on Analysis and Recommendations. It is based on 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 are outlined in detail.

The D6.10 deliverable introduces and reports on the first work around the EXERTER fifth yearly scenario, *Influences to EU civil security emanating from conflict zones*. It describes the scenario, the work on requirements, needs and recommendations, and the work done on standardisation and exploitation.

The report aims to produce tangible output useful 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: *Influences to EU civil security emanating from conflict zones*. It provides the updated user requirements, based on discussions with practitioners and other stakeholders, and an analysis of the research and initiatives in standardisation and certification that are ongoing in the field. It also includes aspects of the issue presented and discussed during the annual conference.

Two related reports exist that are security classified and contain requirements, needs, and recommendations connected to this year's scenario to different degrees of detail: 1, D6.17 (EU-RE) "EXERTER 10th report on innovation, standardisation and exploitation within SoE" that contains recommendations connected to this year's scenario; 2, D6.18 (EU-CO) "EXERTER 10th report on innovations, standardisation and exploitation within SoE" The information is believed to be security sensitive. The level of detail is high and may include detailed gaps or capabilities.

In an appendix to this report is a public summary of the achievements concerning the scenario. EXERTER will distribute this summary also to a broader audience interested and active in the field.

Contents

Summary 3
Contents 4
1 Introduction 5
1.1 Background 5
1.2 Objectives and content of the report 6
1.1 Outline of the report 6
2 Year 5 scenario 7
2.1 Development forced by need 8
2.1.1 Artfully concealed explosives 8
2.1.2 IED based on Pyrotechnics 8
2.2 Development created by opportunity 9
2.2.1 Explosive Remnants of War 9
2.2.2 Terrorist training 9
3 Identified requirements and gaps 10
3.1.1 Prevent 10
3.1.2 Detect 10
3.1.3 Mitigate 11
3.1.4 React 11
4 Research review 12
4.1 Introduction 12
4.2 Progress 12
4.2.1 Prevent 12
4.2.2 Detect 13
4.2.3 Mitigate 14
4.2.4 React 15
5 Stakeholder requirements workshops 17
6 Standardisation and innovation in the explosives security domain 18
6.1 Identified opportunities for standardization and certification of security of explosives 18
6.1.1 Observations 18
6.1.2 Opportunities and recommendations 19
7 Exploitation 20
7.1 Virtual Workshops 20
8 EXERTER Conference and webinar, outcomes 22
9 Conclusions and recommendations 24
10 Appendix 25
10.1 Public summary 25

1 Introduction

1.1 Background

EXERTER connects 20 practitioners from 13 EU Member States 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 (SoE). The EXERTER network's core brings together experts from Law Enforcement Agencies (LEA), 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 can exploit the innovations into products
- Enhancing practitioner's operability by supporting standardisation and certification bodies as well as regulators with standardisation and certification priorities to facilitate comparison of SoE products and procurement
- Enabling long-term cooperation among explosives specialists in the security area beyond EXERTER

Though being an independent network in terms of expertise, the goal of EXERTER is 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 is expanded during the project to include relevant stakeholders. In addition, a more comprehensive network is included in all dissemination activities. The project's results and outputs are through yearly conferences, workshops, webinars, newsletters, and other interactive activities.

In EXERTER, the yearly scenarios are used as a framework to highlight different aspects of the explosives threat and as a base to work with these aspects within research, innovation, standardisation, and exploitation. Four individual counter-attack domains are continuously pursued in the yearly scenarios; these are referred to as Prevent, Detect, Mitigate, and React, see Figure 1. The countermeasures under these four domains differ technically and operationally. Primarily, they have different sets of users and stakeholders, thus setting a broad scope for the EXERTER network.

Figure 1: The counter-attack domains addressed by EXERTER.

1.2 Objectives and content of the report

This report is the tenth of the 6-monthly Deliverables on analysis and recommendations in the EXERTER project. It aims to summarise and analyse information on requirements, innovations, standardisation, and exploitation related to the yearly scenario and present tangible results for the stakeholders.

This year's scenarios have the theme "Influences to EU civil security emanating from conflict zones", and the scenarios and identified key elements are described in Chapter 2 of this report. The scenarios are 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 individual counter-attack domains, 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. Largely, they have different sets of users and stakeholders, thus setting a broad scope for the EXERTER network.

1.1 Outline of the report

This report starts with an overview of the last year's set of scenarios, and summarises the discussions about requirements, gaps, and procedures. It highlights relevant research projects and reviews material that EXERTER has used as input for the standardisation and certification work. It also describes the work performed to capture the product development in industry and by manufacturers; this allows getting their view on how different procedures are working and where there is room for improvement.

Furthermore, the content and outcome of the EXERTER annual conference is described, and the report concludes with an analysis and recommendations.

In an appendix to this report is a public summary of the achievements concerning the scenario. EXERTER will distribute this summary also to a broader audience interested and active in the field.

Two related reports exist that are security classified and contain requirements, needs, and recommendations connected to this year's scenario to different degrees of detail: 1, D6.17 (EU-RE) "EXERTER 10th report on innovation, standardisation and exploitation within SoE" that contains recommendations connected to this year's scenario; 2, D6.18 (EU-CO) "EXERTER 10th report on innovations, standardisation and exploitation within SoE" The information is believed to be security sensitive. The level of detail is high and may include detailed gaps or capabilities.

2 Year 5 scenario

Each year, EXERTER focuses the discussions, issues and suggestions around a set of scenarios to keep the discussions focused and find new challenges. The description of the fifth scenario scope is presented in this chapter and is available in EXERTER D6.9.

The previous sets of scenarios used have been on VBIEDs and HMEs (year 1), explosive attacks in the public transport system (year 2), person-borne IED (year 3), criminal use of explosives (year 4), and now *Influences to EU civil security emanating from conflict zones*.

Input from practitioners regarding themes for the upcoming year's scenario was requested in December 2021. The topic "future and emerging threats" was suggested as a possible theme and several partners expressed their interests for this idea. The input from different partners and practitioners were discussed in meetings with work-package (WP) leaders and Counter-attack coordinators (CACs) in February and March 2022. The title of the 5th year's scenarios and the content of the scenarios were the focus of the discussions.

National security threats have escalated due to recent technological advances and political unrest. An increase in the use of explosives in attacks has created a global security challenge. The online environment has been instrumental in fostering radicalisation, leading to an uptick in lone actors associated with violent extremism. The COVID-19 pandemic has further intensified these risks by shaping extremist narratives, particularly among isolated and vulnerable individuals. Geopolitical shifts, such as the conflict in Ukraine, have also influenced EU's security due to potential violent reactions, mobilisation, and weapon transfers. It is crucial to monitor these developments and collaborate internationally to mitigate these threats. This report aims to identify potential threats and attack strategies by examining past events and current global situations, with a focus on the use of explosives.

EXERTER D9.2 examines past events and the current global evolving situations, to project and identify potential threats and attack strategies concentrating on the deployment of explosives. It provides an overview of the terrorist and organised crime threats, adopting a historical and legal perspective, exposing vulnerabilities that become enablers for attack strategies. This report is connected to the EU-RE classified report D9.4, Updated threats and attack strategies – Annex 1, and the EU-C D6.18, where more details can be found.

The topic chosen for this year is broader than earlier and, unfortunately, highly relevant. The basics for this scenario are that events in conflict zones are driving forces to find new ways to create improvised attacks, information that is transferred to situations outside the conflict zone. That has been historically observed and is likely to continue to influence future modi operandi in Europe.

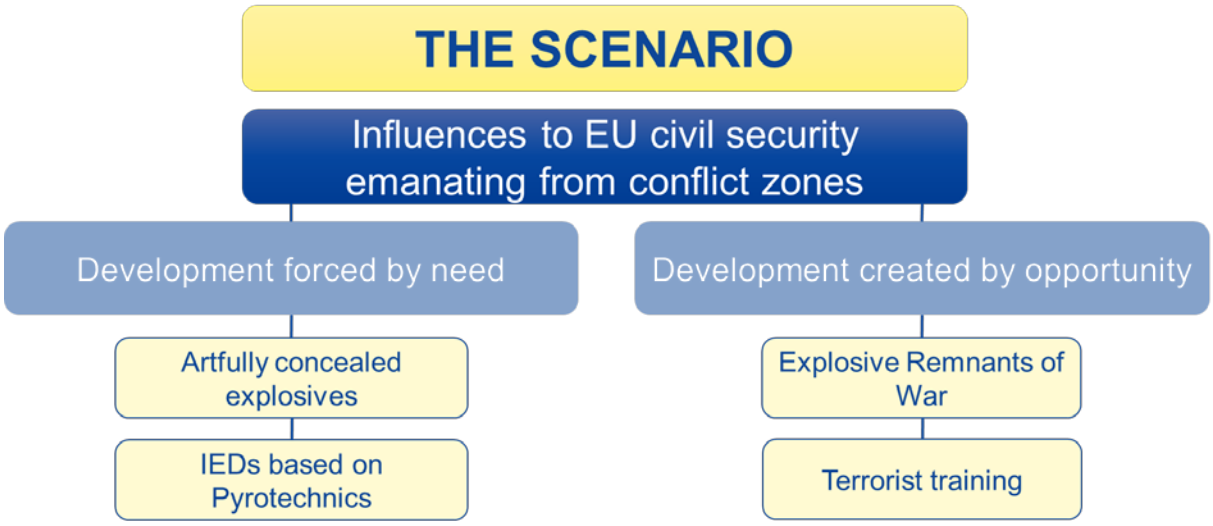


Figure 2: Overview of the scenario. Note that the term "conflict zones" is used in a broad sense

Two sub-topics, “Development forced by need” and “Development created by opportunity”, have been identified as guidance to discussions surrounding this year’s scenario. Details of the sub-scenarios are described below. They are interconnected in many ways; for example, emerging technologies could open opportunities to conceal explosives, but they serve to guide scenario discussions.

2.1 Development forced by need

2.1.1 Artfully concealed explosives

This sub-topic has to do with our adversaries needs to get explosives through customs or security in order to perform an attack. Attackers have been known to counteract security countermeasures and this can be expected to continue.

There have been some interesting cases of “artfully concealed explosives” in the 21st century. The first example was probably the shoe bomber (2001) hiding explosives in his shoes.[1] The 2006 terror plot involved plans to take home-made coloured liquid explosives introduced in unopened drinks bottles on to a series of US and Canada-bound flights from London.[2, 3] Other examples are the underwear bomber (2009)[4] and the printer cartridge bomb plot (2010).[5]

Looking to future possibilities, in 2014 the Al Qaeda described ways, which they claim would make detection more difficult (a.k.a. “the hidden bomb”). It is also quite possible that methods found in the smuggling of illicit drugs will be seen in the future.[6]

Explosives could be coloured and moulded to look innocent or even printed into a desired shape, additionally it could be hidden in different objects, inserted into sealed containers or disturbing substances added trying to prevent detection.[7, 8]

2.1.2 IED based on Pyrotechnics

Unlike the last years scenario focusing on criminal’s misuse of pyrotechnics the aim this year is to cover pyrotechnics based IEDs intended to hurt, kill and engender fear in a larger scale. This sub-topic concerns the use of pyrotechnics based on need due to lacking access to explosives that are more powerful or simply earlier success with pyrotechnics (terrorism).

An example of transfer of the use of pyrotechnics is the bomb construction used in the attack on Boston Marathon in 2013. Both IEDs consisted of pressure cookers concealed in backpacks with low-grade explosives, nails, shards of metal, and ball bearings. The bombs were built with inspiration from Al-Qaida sources.

---

[1] “Richard Reid’s Shoes,” 2020, Accessed: Mar. 28, 2022. [Online]. Available: https://www.fbi.gov/history/artifact-of-the-month/december-2020-richard-reids-shoes

[2] “Liquid bomb plot: What happened,” BBC NEWS, Sep. 07, 2009. http://news.bbc.co.uk/2/hi/uk_news/8242479.stm (accessed Mar. 28, 2022).

[3] “Liquid bomb terror threat failures, archive papers reveal,” BBC NEWS, 2022. https://www.bbc.com/news/uk-scotland-59687706 (accessed Mar. 28, 2022).

[4] “Christmas Day bomber sentenced to life in prison,” CNN NEWS, 2012. https://edition.cnn.com/2012/02/16/justice/michigan-underwear-bomber-sentencing/index.html (accessed Mar. 28, 2022).

[5] “Printer cartridge bomb plot planning revealed,” BBC NEWS, 2010. https://www.bbc.com/news/world-middle-east-11812874 (accessed Mar. 28, 2022).

[6] EMCDDA, “Developments in the European cannabis market,” Luxembourg, 2019.

[7] “Italian police find cocaine hidden inside coffee beans,” BBC NEWS, 2020. https://www.bbc.com/news/av/world-europe-53466854 (accessed Mar. 28, 2022).

[8] A. Navaid, “Creative concealments - the latest lessons from pakistans customs and border control agencies,” Transport Security International, Oct. 2019. https://www.tsi-mag.com/creative-concealments-the-latest-lessons-from-pakistans-customs-and-border-control-agencies/ (accessed Mar. 28, 2022).

2.2 Development created by opportunity

2.2.1 Explosive Remnants of War

The security situation in Europe has drastically changed with Russia's attack on Ukraine and even a conservative assessment could imply a similar situation as after the war in Yugoslavia (which is still feeding criminals with weapons and explosives). How the circumstances will be when the war ends is impossible to discern yet but there could be openings for exploitation to support Criminal and Terrorism related activities.

2.2.2 Terrorist training

The terrorist threat on the security of EU remains on a high level according to the latest EU terrorist situation and trend report. Jihadist terrorists have proven their capabilities and intent through previous attacks to create great damage to European populations, and the majority of the convictions and acquittals handled by the European courts last year concerned jihadist terrorism. One of the main concerns are foreign terrorist fighters (FTFs) who originate from or travel to conflict zones where they receive terrorist training and then return to the European nations. In 2021, several FTFs were arrested upon entering the EU for being part of terrorist organisations, for planning/preparing attacks or for training on how to perform attacks.

Training courses also occur online with guidance and material provided by extremist organisations that have experience from war or terrorist camps. HSM have invited Muslims to travel to Somalia to join them and encouraged those who cannot travel to take part of their online training course and to carry out attacks in their respective homelands. The increased time spent online during the covid-19 pandemic along with social isolation increases the risk for vulnerable people to head down the path of extremism. Especially minors, who spend more time online and are easier targets, are at risk - which terrorists are aware of and strategically channel their propaganda through gaming platforms.9 Training also somehow implies that a new threat (modus or technical), could be spread quite fast over an area in the worst case.

[9] Europol, "EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT ," Luxembourg, 2022.

3 Identified requirements and gaps

A thorough examination of historical incidents, partnered with input from EXERTER associates and expert workshop attendees, informs this report's exploration of targets, vulnerabilities, threats, and attack strategies. The readily accessible knowledge and technology, coupled with identified weaknesses (including legal), pose significant challenges for developing countermeasures within an attack's timeline. The growing number of actors involved in acquiring and deploying explosives necessitates vigilant monitoring.

The analysis underscores the global issue of explosives deployment, made possible by swift information exchange and network formation. Thus, to counteract the evolving, multifaceted landscape, international cooperation among agencies and organisations (both state and non-state) is paramount, necessitating a systematic evaluation and gap analysis.

During the scenario discussions, regulations and control of 3D-printed threats were raised, along with other means of prevention towards concealed threats. Once again, the smuggling of explosives and other illicit material was highlighted as a relevant issue, and the importance of an electronic munition catalogue to prevent the spread of ERWs has been emphasized. Detection systems for behavioural patterns and pattern change were discussed, as well as technological and operational challenges in detection. Training for new threats to improve responses to explosive threats was identified as an important need, also enhanced collaboration during post blast investigations and information exchange on emerging threats and previous cases. The identified requirements and gaps is described more in detail in the EXERTER deliverable D2.1 (EU-C) and D6.16 (EU-R).

3.1.1 Prevent

Efforts to prevent concealed explosives should focus on limiting access to printers and precursor materials while requiring registration for purchases. Harmonizing background checks for legal handlers of explosives, such as those in the mining and construction industry, is essential. Collaboration with counter-narcotic forces will improve results and may lead to exploring potential applications in the postal chain. Controlling the spread of legally purchased pyrotechnics, especially across borders, is a challenge that needs to be addressed. Financial support should be provided to encourage people to hand in explosive remnants of war. Enhanced collaboration between agencies countering drug smuggling and war remnants smuggling is vital. Additionally, addressing the problem of terrorist training camps and surveilling foreign fighters upon their return to their country of origin will help prevent potential lone-wolf attacks.

- Limiting access to printers or precursor material and registering purchases.
- Harmonizing background checks for legal handlers of explosives (e.g., mining and construction industry).
- Collaborating with counter-narcotic forces to improve results.
- Exploring possibilities for applications in the postal chain.
- Addressing the issue of controlling the spread of legally purchased pyrotechnics, especially across borders.
- Providing financial support to encourage people to hand in explosive remnants of war.
- Enhancing collaboration between agencies countering drug smuggling and war remnants smuggling.
- Addressing the problem of terrorist training camps and surveilling foreign fighters upon their return to their country of origin

3.1.2 Detect

Detection efforts must involve continuously updating technologies and educating personnel, with a focus on anticipating developments in the Darknet. Concepts for detecting pyrotechnic materials and bomb-making factories should be further developed and implemented. Improving intelligence and detection methods to disrupt smuggling activities is crucial, as is adapting to novel smuggling techniques and training personnel on emerging threats. Improving biometric identification systems will help spot

individuals traveling with different identities. Encouraging closer collaboration between police and the public, such as in sports clubs, can lead to better reporting of suspicious individuals. A centralized database on purchased precursor chemicals should be established to recognize suspicious patterns.

- Continuously updating technologies and educating personnel, anticipating developments in the Darknet.
- Developing concepts to detect pyrotechnic materials and bomb-making factories.
- Improving intelligence and detection methods to disrupt smuggling activities and adapting to novel smuggling techniques.
- Training personnel who use detectors on emerging threats.
- Implementing biometric identification to spot individuals traveling with different identities.
- Encouraging closer collaboration between police and the public (e.g., in sports clubs) for better reporting of suspicious individuals.
- Creating a centralized database on purchased precursor chemicals to recognize suspicious patterns.

3.1.3 Mitigate

Mitigation efforts should concentrate on training first responders to recognize new threats and ensuring that physical protection measures are independent of the type of concealment. From an operational standpoint, high explosives and pyrotechnics should be treated the same. Infrastructure known as targets for attacks, such as ATMs, should be placed in locations where their destruction limits collateral damage.

- Training first responders to recognize new threats.
- Ensuring physical protection is independent of the type of concealment.
- Treating high explosives and pyrotechnics the same from an operational standpoint.
- Placing infrastructure known as targets for attacks (e.g., ATMs) in locations where destruction limits collateral damage.

3.1.4 React

In response to concealed explosives, post-blast investigations must be improved, with a focus on forensics and information sharing. Combining efforts to follow and anticipate developments in the scene is crucial. Enhanced information sharing across borders will increase the knowledge of bomb technicians and improve statistics for earlier trend recognition. Pre- and post-blast forensics should be utilized to trace the origin of used explosives and other components. EODs must be prepared for emerging threats, and the publication of HME synthesis in scientific literature should be limited.

- Improving post-blast investigation concerning forensics and information sharing.
- Combining efforts to follow and anticipate developments in the scene.
- Enhancing information sharing across borders to increase knowledge of bomb technicians and improve statistics for earlier trend recognition.
- Utilizing pre- and post-blast forensics to trace the origin of used explosives and other components.
- Preparing EODs for emerging threats.
- Limiting the publication of HME synthesis in scientific literature.

4 Research review

4.1 Introduction

Within EXERTER, an overview of research projects is made, identifying completed and ongoing national, European, and international Security of Explosives (SoE) projects that can help in the fight against terrorist attacks. Relevant research projects are screened with the aim of finding solutions to user needs and closing gaps. Each year, projects related to the set of scenarios are identified. They are further studied in each of the four counter-attack domains PREVENT, DETECT, MITIGATE and REACT in order to identify relevant solutions or needs for further research.

4.2 Progress

The year 5 scenario "Threats for EU civil security emanating from conflict zones" is divided into four subtopics, namely: Artfully concealed explosives, IEDs based on Pyrotechnics, Explosive Remnants of Wars and Terrorist training. The full description of this scenario can be found in D6.8.

4.2.1 Prevent

Since the yearly overall topic is immediate and emerging threats, the ongoing project LAW-GAME would be interesting to follow. LAW-GAME is creating interactive gaming technologies that aim to train police officers in virtual crisis scenarios, among other things. The developing training tool could prepare security personnel in extreme situations and enhance the prediction of criminal actions e.g. terrorist attacks as well as improve the threat response.

For "Artfully concealed explosives", one could consider projects preventing HME production. However, this project type has been lifted several years during the EXERTER project. Project UNCOVER aims to enhance intelligence work. Uncovering plans for an attack involving a concealed explosive charge could be essential before the transportation and execution phase.

It has been proven difficult to prevent the smuggling of ERWs and pyrotechnics across borders. The research projects ANITA, ENTRANCE, and PARSEC deal with smuggling and improving checkpoint security. The latter tackles the detection challenge and will develop and test three new technologies to stop criminals and terrorists from using postal services as transportation means for illegal and dangerous parcels.

The initiative PROHETS that ended in 2021 dealt with the prevention of radicalisation, as does the ongoing project CounteR. The toolkit and platform developed in these projects aim to aid in preventing radicalisation and reducing the number of young men trained to become terrorists.

- **LAW-GAME** 2021-2024: An Interactive, Collaborative Digital Gamification Approach to Effective Experiential Training and Prediction of Criminal Actions; it is a serious game that recreates the real world to train police officers on the procedure through gamification technologies.
- **UNCOVER** 2021-2024: Development of an efficient steganalysis framework for uncovering hidden data in digital media; it aims to fill existing gaps in the ability of Law Enforcement Agencies to detect hidden information using steganalysis.
- **ANITA** 2018-2021: Advanced tools for fighting oNline Illegal TrAfficking; it develops a knowledge-based user-centred investigation system to analyse online and offline content for fighting illegal trafficking.
- **ENTRANCE** 2020-2023: EfficieNT Risk-bAsed iNspection of freight Crossing bordErs without disrupting business; it aims to develop and validate a comprehensive toolbox for risk-based non-intrusive inspection of cross-border freight movements, validated by five field trials.
- **PARSEC** 2022-2025: Parcel and Letter Security for Postal and Express Courier Flows; it aims to develop three non-intrusive detection technologies and combine them into a detection architecture to stop the abuse of postal and express courier flows.

- **PROHETS** 2018-2021: Preventing Radicalisation Online through the Proliferation of Harmonised ToolkitS; it will redefine new methods to prevent, investigate and mitigate cybercriminal behaviours by developing an EU-wide adaptive SECURITY MODEL.
- **CounteR** 2021-2024: Privacy-First Situational Awareness Platform for Violent Terrorism and Crime Prediction, Counter Radicalisation and Citizen Protection; it aims to prevent future terrorist attacks by bringing data from dispersed sources into an early alert platform for data mining and prediction of critical areas.

4.2.2 Detect

MiRTLE is a low-cost threat detection system by Radio Physics Solutions that can detect concealed weapons and explosives up to fifty metres away. CONSORTIS aims to develop a stand-off concealed object detection demonstrator using a dual-frequency submillimetre-wave video camera and active 3D imaging radar system. TERASCREEN seeks to create a security screening technology for border checks using passive and active operation at several Terahertz frequencies. VMEWI3 aims to develop a technology demonstrator using remotely operated unmanned ground vehicles to detect indirect indicators of IED presence. MUSICODE will develop new unmanned ground vehicle stand-off capabilities to detect IED components. CONFIDENT aims to develop technology demonstrators using remotely operated platforms to confirm and identify IED components and provide complementary early warning capability. MKD proposes a new system of landmine detection based on unmanned aerial vehicles. COSMIC proposes a three-stage detection system with eight CBRNE sensors to detect CBRNE materials hidden in shipping containers and vehicles.

- **MiRTLE** (Next generation, high performance, long range, standoff, concealed threat detection system to protect European citizens and critical infrastructure); it is an autonomous, low-cost threat detection system by Radio Physics Solutions that can detect concealed weapons and explosives up to 50m range, with an aim to capture an 8% market share and generate €161m in cumulative revenues by 2025.
- **CONSORTIS** (Concealed Objects Stand-Off Real-Time Imaging for Security): it aims to develop a stand-off concealed object detection demonstrator for European mass-transit markets and infrastructure security using a dual-frequency passive submillimetre-wave video camera and active 340 GHz 3D imaging radar system with automatic anomaly detection algorithms to improve automation and mitigate privacy issues.
- **TERASCREEN** (Multi-frequency multi-mode Terahertz screening for border); it aims to develop a security screening technology for border checks that combines automatic detection and classification of body-borne threats using passive and active operation at several Terahertz frequencies to improve efficiency and security.
- **VMEWI3** (Vehicle Mounted Early Warning of Indirect Indicators of IEDs (EDA)); it aims to develop a technology demonstrator using remotely operated unmanned ground vehicles with a multi-camera head to detect indirect indicators of IED presence, providing early warning capacity while moving at a speed of 20-30 km/h.
- **MUSICODE** (UGV stand-off multi-sensor platform for IED component detection (EDA)): This project will develop new unmanned ground vehicle (UGV) stand-off capabilities for detection of IED components by using remotely operated multisensory platforms.
- **CONFIDENT** (Confirmation, Identification and Airborne Early Warning of IEDs (EDA)); it aims to develop technology demonstrators using remotely operated platforms (robot and UAV) to confirm and identify components of IEDs, including CBRN payloads, and provide complementary early warning capability, with the UAV used for airborne early warning.
- **MKD** (A drone to clear minefields): The EU-funded MKD project proposes a new system of landmine detection based on unmanned aerial vehicles (UAVs). The Mine Kafon Drone system is a safe, reliable, efficient, fast and cheap solution. It maps and scan entire areas to find the mines and then places a small detonator on every detected mine.
- **COSMIC** (CBRNE Detection in Containers); it proposes a novel approach to detect CBRNE materials hidden in shipping containers and vehicles at border crossings and critical

infrastructure entrances. It includes a three-stage detection system with eight innovative CBRNE sensors developed by technology partners Lingacom, Technion, BGU, and CNB-CSIC/Yale. Atos developed the software for end-users to access sensor data, analytics software, risk assessments, and alarms through web-enabled devices.

- The Department of National Defence and the Canadian Armed Forces (DND/CAF) seek to improve stand-off detection of concealed explosives in order to mitigate the threat to soldiers operating in high-risk environments. As a result, following projects were funded in the context of detecting concealed explosives:
    - CASCADE Combining Al with SWIR Camera for Automatic Detection of Explosives. Innovator: MDA Systems Ltd.
    - Ultra-Sensitive MEMS PhotoAcoustic Spectroscopy for Real-Time Explosive Detection. Innovator: NxtSens Microsystems
    - Microwave-based Nose Radar System toward Standoff Detection of IED. Innovator: UBC
    - Detection of Concealed Explosives by Extraction and Classification of Micro-Doppler Signatures Arising from Induced Acoustic Vibration. Innovator C-Core

4.2.3 Mitigate

Structural and design measures that mitigate explosion effects are available and have been investigated in various research projects. The specific applicability of each action depends on the location of interest, and a cost-benefit analysis should be conducted. During the design phase of places or buildings, fundamental mitigation aspects, such as safeguarding the distance between the target and potential attack, can be considered. Hazards from fragmentation can be reduced using blast-resistant components and appropriate separation of places. Organisational measures that can minimise explosion effects include reducing people's exposure, evacuating people, and training first responders. First responders do not know what kind of explosive might be inside the IED. Instead, the response to an attack depends on the location and surroundings of the IED.

Physical and organisational mitigation measures for EU civil security depend on the location and surroundings of IEDs rather than the type of IED. Research projects such as AURIS, ELASSTIC, SPIRIT, SUSQRA, and TACTICS have developed tools, technologies, and methods to enhance security, reduce damage, and improve attack response.

AURIS established a security management system for critical infrastructure and building health monitoring. ELASSTIC focused on building design and sensor technology. SPIRIT developed tools to enhance the security of large buildings against terrorist threats. SUSQRA aimed to create software for post-blast IED damage evaluation. TACTICS developed tools for improving security forces' ability to prevent and handle urban attacks.

For the 5th year scenario, "influences to EU civil security emanating from conflict zones", the effectiveness of structural- and design mitigation measures strongly depend on the physical hazard originated from the IED and specifically the kind of explosive used. The physical hazard (blast and fragmentation) of IEDs that are based on pyro techniques or based on new casing materials (e.g. through additive manufacturing of synthetic materials) is almost unknown, respectively; there are no research projects that specifically look on these aspects. However, it can be assumed, that the physical violence of such IEDs is equal to- or less than the ones of IEDs using typical high-explosives with metal encasements. As such, a differentiation from physical mitigation measure options according to the kind of IED is not targeting, necessary, or applicable at all. With respect to the physical mitigation of explosion effects, the IED type is less relevant compared to the target of the attack.

Also, with respect to organisational mitigation measures, as evacuation procedures or IED neutralisation, a differentiation between general, more commonly known IEDs, and the IEDs related to the year 5 Scenario, is neither targeting nor applicable, as first responders during an attack do not know what kind of explosive might be inside the IED. Also in this case, the response to an attack is not connected to the kind of an IED, but the location and surrounding where it is placed. As a consequence,

physical and organisational mitigation aspects from the following research projects could be transferred to the 5th year scenario:

- **AURIS** (Autonomous risk and information system for structural analysis and health monitoring of security-relevant buildings): In AURIS a security management system of critical infrastructure was established, also considering monitoring of building health and progressive collapse.
- **ELASSTIC** (Enhanced Large Scale Architecture with Safety and Security Technologies and special Information Capabilities); it focused on building design concepts and sensor technologies for safety, security, and resilience of building complexes against 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.
- **SUSQRA** (Schutz vor Unkonventionellen Sprengvorrichtungen – Charakterisierung und Quantitative RisikoAnalyse, English transl.: Protection against IEDs – characterization and quantitative risk analysis); it aimed to develop software for forensic post-blast IED damage evaluation, useful for improving infrastructure protection and security measures.
- **TACTICS** (EU FP7: Tactical Approach to Countering Terrorists in Cities); it developed tools and methods to improve security forces' ability to prevent and handle urban attacks, focusing on CCTV and threat management.

4.2.4 React

To REACT to the terrorist attack timeline requires improved collaboration and communication between European forensic and research institutes and first responders, police, law enforcement, and the judiciary. Projects such as ACRIMAS, AUGGMED, CAST, XClanLab, RISEN, ROSFEN, BRIDGE, DARIUS, DirtyBomb, GIFT-CBRN, and PRACTICE aim to facilitate this cooperation by providing training for coordinated and rapid response to attack scenarios, enabling first responders to assess a crisis without endangering themselves, developing solutions for stable and uniform crisis management, and exchanging expertise regarding new solutions necessary to civil security. These projects also prepare for realistic threats for example dirty bombs, attacks on critical infrastructure, and remote-operated vehicle attacks.

AUGGMED, CAST offer a unique crisis training that is indispensable for coordinated and rapid dealing with attack scenarios. The projects XClanLab, RISEN or ROSFEN provide probate measures to enable first responders to assess a crisis situation without endangering themselves. Whereas the project BRIDGE offers solutions for a stable and uniform crisis management as an indispensable basis for adequate reacting in attack scenarios. DARIUS aims towards the exchange of expertise regarding new solutions that are important to be aware of the state of art of tools. Projects like DirtyBomb, GIFT-CBRN, PRACTICE are very important for preparation realizing the fact that dirty bombs became a slightly more realistic threat than in the recent past. The same importance is attributed to the projects EMILI or VASA, since threats/attacks towards critical infrastructure become an increasingly more realistic threat as well as attacks by remote operated vehicles (drones) (RESPONDRONE).

- **ACRIMAS** (Aftermath Crisis Management System-of-systems Demonstration): This project aims to set up a large-scale European demonstration programme for crisis management, encouraging collaboration and cooperation across member states.
- **AUGGMED** (Automated Serious Game Scenario Generator for Mixed Reality Training): The aim of AUGGMED is to create a serious game platform that supports training for different organisations responding to terrorist and crime threats.
- **CAST** (Comparative assessment of Security-Centered Training Curricula for First Responders on Disaster Management in the EU): This project will comparatively assess disaster management training curricula for first responders in EU member states, deriving from international best practices.

- **XClanLab:** Focusing on illicit bomb factories, XClanLab aims to develop an app for first responders to ensure safety and efficient communication with experts.
- **RISEN** (Real-tIme on-site forenSic tracE qualification): aims to develop real-time contactless sensors for onsite forensic trace detection and interpretation, producing interactive 3D crime scene models.
- **ROSFEN** (Rapid On-site Forensic Analysis of Explosives and Narcotics): developed a forensic platform for rapid, onsite detection and lab-quality analysis of explosives and their precursors.
- **BRIDGE** (Bridging resources and agencies in large-scale emergency management): strives to improve crisis and emergency management in the EU by developing technical and organisational solutions.
- **DARIUS** (Deployable SAR Integrated Chain with Unmanned Systems): aims to create a technological framework for sharing innovative tools and resources among manufacturers, departments, and agencies in the Search and Rescue sector.
- **DirtyBomb** (Increased preparedness to CBRN incidents via first responders' joint exercises): This project focuses on enhancing preparedness for "dirty bomb" terrorist attacks, identifying critical points to improve and developing relevant training materials.
- **GIFT-CBRN** (Generic Integrated Forensic Toolbox for CBRN): aims to develop a toolbox for investigating CBRN incidents, including procedures, sampling methods, and laboratory methods.
- **PRACTICE** (Preparedness and Resilience against CBRN Terrorism using Integrated Concepts and Equipment): goal is to enhance EU preparedness and resilience to CBRN terrorism attacks, addressing fragmentation in technology, procedures, methods, and organization.
- **EMILI** (Emergency management in large infrastructures): aims to develop new generation control systems for large critical infrastructures such as power grids, telecommunication systems, airports, and pipelines.
- **VASA** (Visual Analytics for Security Applications): applies visual analytics to disaster prevention and crisis response, focusing on critical infrastructures. It aims to produce a demonstrator for rapid visual evaluations of complex crises.
- **RESPONDRONE** (Unmanned aircraft systems platform to support situation assessment for first responders): aims to create an integrated drone system for first responders to enhance their situation assessment capacity and protection, simplifying operations management.

5 Stakeholder requirements workshops

Workshops are held annually with stakeholders, including law enforcement agencies, government, academia, and research, to collect input on requirements, needs, and gaps and discuss best practices and ideas. Details to these workshops are described in EXERTER D6.9.

The workshops were face-to-face events for the first two years of EXERTER, including project partners and EXERTER network stakeholders. For years three and four, the workshop procedure had to be adapted to the restrictions of the ongoing Covid19-pandemic, and therefore, several smaller workshops were held nationally.

This year a workshop was held physically in Belfast, Northern Ireland, 25–26 October 2022. It had 47 participants from 27 different organisations, and focus was to share experiences connected to the scenarios, discuss needs and share recommendations and ideas.

The discussions from the groups on needs, requirements and recommendations were summarised and analysed, and form the basis for the continued EXERTER work during the project's 5th year. The discussion during the workshop revolved around the four subtopics introduced above.

The outcomes of the discussions are classified EU-RE and were collected in the deliverable EXERTER D6.16.

6 Standardisation and innovation in the explosives security domain

The work has been continued in EXERTER to monitor standardisation initiatives and to extract and list prioritisation areas for standardisation within SoE.

The current year's topic, "*Influences on EU civil security emanating from conflict zones*", and its sub-topics are not topics that easily fit into the Standardisation domain. The common denominator, however, is the fact that "information sharing" within the C-IED community about new security threats emanating from conflict zones is key. In addition, it is not obvious that C-IED agencies in Europe, and even within one country, share information in a standardised way. The sensitive nature and (most of the time) classification of this information make information sharing more difficult.

During the EXERTER stakeholder workshop, where the different sub-topics (see chapter 2) were discussed by end-users, difficulties in information sharing were also frequently mentioned as an obstacle to tackling influences on EU civil security emanating from conflict zones, underpinning the need. During the last months of the project, EXERTER focused on possibilities to standardise information sharing further between EU nations and between agencies. Where standardisation is not deemed possible, the options for sharing "best practices" was explored.

6.1 Identified opportunities for standardization and certification of security of explosives

Within the EXERTER project, two online workshops/webinars have been organised dedicated to standardisation in the field of security of explosives. This chapter contains the findings of these workshops/webinars. The theme of the first webinar, organised in October 2021 in conjunction with EXERTER WP5, was "Is standardization an enabler for exploitation of innovations in security against explosives?" The aim of the webinars was to invoke discussion and connect attendees (a variety of explosive security professionals: law enforcement, policy makers, scientists, equipment manufacturers, R&D institutes and other stakeholders) during the breakout sessions.

6.1.1 Observations

1. As early as 2007, the need for standardisation in the field of security of explosives was identified. See for instance objectives 3.2.1, 3.4.1, 3.4.2, 3.4.3 and 3.4.4 in[10]:
   - "Develop minimum detection standards based on relevant scenarios and threat assessment. These standards should be updated as technology evolves"
   - "Create a European wide certification scheme for explosives detection solutions"
   - "Create a European wide testing scheme for explosives detection solutions. Under the scheme relevant authorities and institutes would be able to exchange test results"
   - "Create a European wide trialling scheme for explosives detection solutions. Such a system should be supported by an EU programme and should allow for conducting performance trials under realistic conditions in same or similar scenarios"
   - "Assess the need for the development of standardized procedures and processes concerning certification, testing and trialling processes"
2. These objectives are followed up by the NDE in their CTT report, in which a clear scheme was presented for certification, testing, and trialling. In addition, the ERCIP initiatives resulted from the action plan in 2007.
3. Later on, the HECTOS project was executed, following a call in the EU FP7 program. Where the previously mentioned initiatives focussed mainly on the detection of explosives, this project provided a comprehensive scheme to come to certification of a much wider variety of security products.

[10] "EU Action Plan on Enhancing the Security of Explosives", Doc 8311/08, Council of the European Union, 11 April 2008

4. Even though some results from for instance ERNCIP found their way into EN or ISO standards, much work in their Technical Committees seems to be executed isolated from other initiatives.
5. The field of aviation security is a special field with respect to standardisation end certification. It is one of the most mature fields, but is also perceived as complex, slow and expensive. Nevertheless, it may serve as an example of successful implementation of standardisation.
6. The speed of developing standards is a of concern. With the DG Home initiative as a clear example, where it took several years to come to a standard for x-ray equipment image quality, of how slow such a process can be.
7. The approach of developing standards seems to be fragmented, with many initiatives, some of them repeating previous work. Coordination on a European level seems missing.
8. Most initiatives on a European or trans-national level are in the domains of explosives detection and blast resistant structures, mainly glass and windows. Other fields are less represented, but the assumption is than in the fields of prevent and react, standardisation takes place more on a national level.
9. From the workshops and other discussions within EXERTER a clear need for better (classified) information exchange is desired. This means exchange of intelligence and information between member states, but also between agencies and even within organisation. Exchange of classified information with industry, including SMEs, R&D, and universities is perceived difficult, or even impossible, hindering innovation.

6.1.2 Opportunities and recommendations

Based on the observations in the previous paragraph, the following opportunities and recommendations for standardization and certification in the field of security of explosives are identified:

1. Use the existing information and schemes developed in previous projects. Especially the HECTOS proposed schemes can be used almost directly to develop and implement standards, but also the NDE scheme, which also involves trialling of new technologies, can enhance innovation.
2. Coordinate the development of standards and certification on a European level. Make sure that it leads to a coherent set of standards, throughout prevent, detect, mitigate, and react domains.
3. The performance standards should reflect on one hand the ambition, derived from the level of inferred security provided by a technology (or method), and on the other the current and near future realizable technical performance. The resulting performance standards (current and future tiers) are, therefore, attractive to industry and SMEs because they represent a realistic market outlook, and the streamline competition on performance.
4. Pay special attention to the exchange of classified information with innovators and enable strong interaction between innovators, end-users, and policy makers. This ensures that products will better meet expectations of end-users and requirements from potential regulators.

7 Exploitation

This chapter summarises the most relevant activities of EXERTER that have been carried out concerning–support to academia and SMEs for industry and user collaboration and exploitation. A market research was conducted on the state of the art of security of explosives' (SoE) equipment, which expanded the data collected in previous projects (e.g., the FP7 HECTOS project, H2020 ENTRAP, European Reference Network for Critical Infrastructure Protection – ERNCIP), and providedg an updated and thorough overview.

To establish industry, academia, and research centre contacts, a thorough market assessment was performed, aiming to involve the most suitable actors in our project. A series of interviews and surveys were planned, with information collected via web-forms instead of physical cards. These forms were sent out twice, in June 2021 and December 2022.

To understand how research prototypes can become market-ready products, three types of work were undertaken: a market screening of equipment used in the field of security of explosives, the development of a practitioner's network for exploitation of innovations, and an appraisal of the situation. In the market screening, equipment was categorized in an Excel spreadsheet. This process included updates to categories based on new literature and usability for all scenarios. A compact overview of market technologies was also created, highlighting important manufacturers and cost estimates.

For the network development, a database was created based on the categorized one-pagers. EXERTER contacted manufacturers to gather information about current innovations and market expansion plans. Personalized emails were sent to relevant companies, directing them to the EXERTER webpage and a web form for detailing their market challenges. In the appraisal of the situation, an analysis was performed on collected data. It provided a comprehensive view of the state of the art in the field of security of explosives and the EU's situation in combating terrorist threats. This analysis identified key companies, countries, and issues, as well as strengths, weaknesses, opportunities, and threats in the EU related to the field.

Additionally, the database provided information on European test centres' locations and capabilities, and academic research and development activities. The tool needs to be kept updated to identify researchers and industries that could commercialise technology to fill the identified requirements and gaps.

The primary objective of this work was to streamline the interaction between academia, industry, researchers, and end-users. It is of vital importance that prototypes are developed with the end-users' needs in mind, evolving into readily available products. The majority of this equipment is designed to assist in combating explosive threats.

7.1 Virtual Workshops

The EXERTER consortium has hosted three virtual workshops, or webinars, as part of a series centred on uniting all participants in the European Security R&I ecosystem to address matters related to exploitation, standardisation, and certification. This method proved successful in providing tangible instances of gaps in the SoE issue.

The first webinar, held on 4th October 2021, discussed standardising innovations and covered the entire innovation cycle as described in D6.8.

The second webinar, "Processes and Technology supporting the Security of Explosives," took place on 9th December 2022. It offered presentations and a Q&A session with an audience of diverse security professionals (chapter 6).

The Stakeholder requirements workshops identified crucial technologies for future development. Funding for these technologies can come from various sources, including governmental bodies and venture capitalists. Technology companies, academia, and researchers participated actively in the webinars. Some examples, which came up was that a participant mentioned the challenges in detecting multiple threats and the need for funding in the sensing field. It was also mentioned that public funding

initiatives like Horizon Europe have improved market prospects for new technologies. Discussions revealed that certification processes can sometimes be slow and expensive, and that technology often precedes regulation. The participants also lifted that outdated regulations need revision, and future professionals must learn about protecting against terrorist threats. Confidentiality of end-user information can limit the understanding of user needs.

Agility is key in the evolving explosive security field, requiring collaboration across all parties. There's a suggestion for an agency to bridge technical knowledge and law enforcement needs across Europe.

As a conclusion, it is believed that the creation of an eco-system including all stakeholders could accelerate innovations in Security of Explosives. It would also be beneficial to try to find a way to open the ecosystems to companies outside the European Union, since certain pieces of the innovation puzzle can only be found beyond our borders.

8 EXERTER Conference and webinar, outcomes

The focus of the EXERTER Year 5 scenario and the conference was "Influences to EU civil security emanating from conflict zones". This was exemplified through case studies, recent research and development findings, as well as legal evaluations.

The EXERTER consortium invited experts from various EU, police, research, and military institutions to share their perspectives on managing aspects of the "emanating threats from crisis zones" scenario in relation to the EXERTER domains PREVENT, DETECT, MITIGATE, and REACT. FOI commenced the first day of the conference by introducing the EXERTER project work, underlining the necessity for a network in the Security of Explosives and outlining the conference's key aspects.

EXERTER consortium member BKA introduced the scenario and acted as the conference moderator. A brief overview of the Year 5 scenario "Influences to EU civil security emanating from conflict zones" was given, highlighting the main influences from crisis zones like "development forced by need", with the themes "IEDs based on pyrotechnics" or "artfully concealed explosives". The second area "development created by opportunity", was further divided in "explosive remnants of war" and "terrorist training".

Subsequent presentations included the following:

- The Advisor to the EU Counter-Terrorism Coordinator who discussed the catalysts, legal and political future challenges in context with terrorism.
- An EXERTER consortium member, FOI who introduced the results of the EXERTER End-User Workshop 2022 on the scenario "Threats for EU civil security emanating from crisis zones". The workshop took place in Belfast as a physical event and was hosted by the EXERTER Consortium member PSNI.
- The joint presentation of the EXERTER Consortium members INTERPOL and KEMEA addressed the emerging global explosives threats, the evolution of threat and attack strategies.

The second day of the conference covered:

- A representative of the Dutch Policeacademie showed, how information awareness and understanding for using anticipatory intelligence could lead to being two steps ahead in C-IED efforts.
- The Federal Institute for Materials Research and Testing (BAM) informed about the numerical analysis of structures under blast loading, discussing scopes and challenges for a technical-safety assessment. They figured out, why reliable numerical simulations were an effective alternative option in this field.
- The presentation of the NATO Counter-Improvised Explosive Devices Centre of Excellence (C-IED CoE) dealt with the dynamics on the use of explosive-laden unmanned aircraft systems. This was supported with numerous examples from conflict zones.
- GEOMAR Helmholtz Centre for Ocean Research gave an overview of the amounts of explosive remnants of the war in the Northern and Baltic Sea and the herewith connected environmental pollution as well as the opportunities of illegal collection of remnants of war.
- A representative of the Defensie CBRN Centrum of the Netherlands commented on potentials and limits of Technical Exploitation as instrument of information retrieval in conflict zones with the focus on the Level 2 Chemical Exploitation in the Joint Deployable Exploitation and Analytic Laboratory (JDEAL).
- The presentation of the United Nations Office on Drugs and Crime (UNODC) focused on the best practices for Security Architecture in the fight against terrorism but likewise the challenges of implementing it effectively.
- A representative of the European Commission Joint Research Centre Safety and Security of Buildings Unit (JRC) gave his expertise on the assessment of blast events, naming several e-tools, especially in the field of simulation, facilitating the protection of the built infrastructure and the public.

- Another representative of the Federal Institute for Materials Research and Testing (BAM) introduced the EU Project ODYSSEUS that aims at preventing, countering, and investigating terrorist attacks through prognostic, detection, and forensic mechanisms for explosives precursors.
- The last conference day was dedicated to the five years of EXERTER project work. After a short introduction by FOI, the work package leader presented their tasks within the project and in the end; a representative of DG Home gave a feedback regarding the EXERTER project. The work package leader of WP2, FOI, commented the objectives of the work package and gave an overview of the selected EXERTER scenarios in connection with the terrorist timeline.
- Fraunhofer ICT as work package leader of WP3 presented the review of research initiatives connected to the yearly scenarios and the four EXERTER domains Prevent, Detect, Mitigate, and React.
- The WP6 task of analysis and recommendation regarding the different yearly EXERTER scenarios in the order of the four EXERTER domains was presented by the work package leader of FOI.
- TNO as work package leader of WP4 presented the issues of standardisation within the EXERTER project as well as the contents and the results of two EXERTER workshops, organised and held by WP4.
- INTA as work package leader of WP5 “Exploitation of innovations”, focused in his presentation on the task WP 5.2 “Support academia and SMEs for industry and end user collaboration and exploitation”. Furthermore, the results of a workshop, a webinar, and the EXERTER project meeting held in Madrid were elaborated.
- The joint presentation of PSNI as work package leader of WP8 and a representative of DG HOME concluded the conference with a closure panel, reflecting and summarising the impact, benefits, and a possible future of the EXERTER project.

During the conference, there was time for questions and discussions directly after each presentation and at the end of each day. The possibility for networking was given and used efficiently during the breaks and the dinners.

Numerous requests after the conference concerning the distribution of the presentation slides or the connection of participants with the speaker were facilitated by the organisation committee.

9 Conclusions and recommendations

In each of the five scenarios and their sub-scenarios, there are a number of ways to prepare for an attack or to intervene during the act. The aim is to prevent the crime in the best case and otherwise minimize the impact of an attack. Some of these options are very specific to the particular circumstances of the attack in question, while others follow certain patterns that occur in different attacks. These patterns should be used at each stage of attack response to achieve the goals of prevention, detection, mitigation, and reaction. Although there are many ways to meet the challenges of attacks, this project has identified those techniques and research results that have proven to be effective for most scenarios. However, it is important to note that each attack is unique and therefore there is no one-size-fits-all solution.

Throughout our research, we have pinpointed a variety of innovative technologies, procedures, strategies, and solutions with the potential to substantially improve public safety.

10 Appendix

10.1 Public summary

Scenario: Influences to EU civil security emanating from conflict zones

The fifth annual report in EXERTER

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

EXERTER
Scenario: Influences to EU civil security emanating from conflict zones -
The fifth annual report in EXERTER

FOI-2017-1045
April, 2023

Photo: FOI

Security of Explosives pan-European Specialists Network

The EXERTER network is a European initiative that seeks to identify and promote innovative methods, technologies, and tools to combat terrorism and serious crime, thereby improving the Security of Explosives. The network brings together a team of experts from Law Enforcement Agencies (LEAs), military institutes, governmental and civilian research institutes, academia, and standardisation organisations.

By fostering the exchange of information on current and emerging threats, operational requirements, and the state of research and innovation, EXERTER empowers practitioners with the knowledge and tools they need to enhance the security of our society. Each year, the network focuses on a series of scenarios related to the Security of Explosives, aiming to identify weaknesses in our response and opportunities for improvement. EXERTER focuses on standardisation, certification, research, innovation, and exploitation.

In its fifth year, the scenarios explored by EXERTER concern influences to EU civil security emanating from conflict zones. This report summarises the network's findings, analyses, and recommendations based on this year's scenarios.

Introduction

EXERTER focuses each year on a specific scenario or set of scenarios identified with input from practitioners and experts. The network then addresses related issues in all four phases of the timeline: PREVENT, DETECT, MITIGATE, and REACT. It examines the requirements, gaps, research, standardisation, and certification activities and strives to implement innovations in all phases.

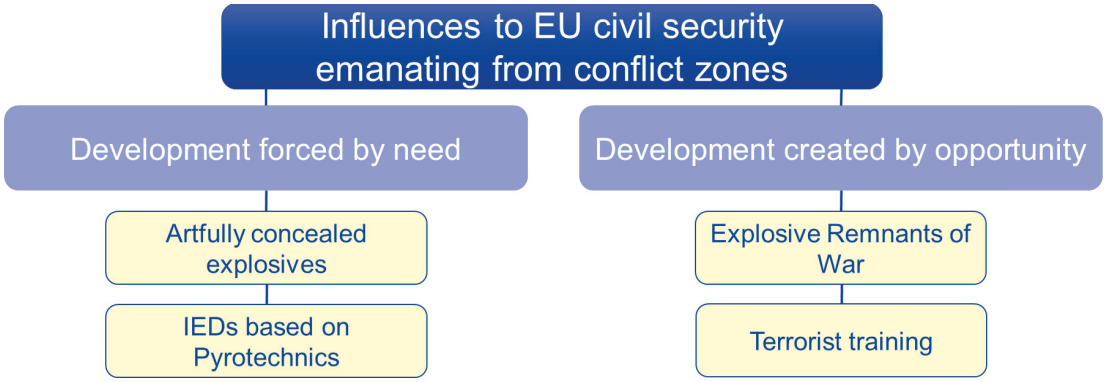
The countermeasures for each domain differ technically and operationally and target different users and stakeholders, setting a broad scope for EXERTER. This report summarises the results of EXERTER's work on scenarios involving influences to EU civil security emanating from conflict zones. It provides an overview of the findings in each counter-attack domain and presents conclusions and recommendations for future directions and needs.

At the start of EXERTER's yearly cycle, the practitioners' requirements and gaps for countering the threat scenario were identified. These were based on analysing input from stakeholders and the expert community. The information was collected in a classified report and was the foundation for the network's continued work.

Scenarios

Influences to EU civil security emanating from conflict zones

Events in conflict zones drive new ways to create improvised attacks, and related information transpires outside the conflict zone. That has been historically observed and is likely to continue to influence future modi operandi in Europe. Here, we focus on four subtopics.



Artfully concealed explosives: Our adversaries must get explosives through customs or security checkpoints to perform an attack. Cases of artfully concealed explosives include the shoe bomber, liquid explosives in unopened drink bottles, the underwear bomber, and the printer cartridge bomb plot. Further possibilities include coloured, moulded, or printed explosives, hidden in objects or containers or mixed with other substances to evade detection. At the same time, techniques for smuggling drugs can be applied to explosives smuggling.

IED based on pyrotechnics: This subtopic concerns using pyrotechnics based on need due to lacking access to more powerful explosives or simply earlier success with pyrotechnics. An example of transfer of the use of pyrotechnics is the IED construction used in the attack on Boston Marathon in 2013.

Explosive remnants of war: Post-conflict environments are exploited to support criminal and terrorism-related activities. Many European countries still have unexploded ordnance and other remnants of World War II that were dumped on land, in lakes, and even in the maritime environment. These explosives have not degraded and remain easily accessible for illicit use. The war in ex-Yugoslavia continues to supply criminals with weapons and explosives, and a similar situation may arise following the conclusion of the Ukraine war.

Terrorist training: Europol's "EU Terrorism Situation and Trend Report" states that the threat of terrorism to the EU remains high. Several individuals were arrested in 2021 after they had received terrorist training in conflict zones. Extremist organisations also provide online training and encourage individuals to attack their homeland. More online activity and isolation during the covid-19 pandemic have increased the risk of radicalising vulnerable individuals. Additionally, suspected terrorists are being trained to produce and use a new explosive material not included in standard detection instruments.

Prevent

The Prevent domain in Year 5 addresses the risks associated with artfully concealed explosives, IEDs based on pyrotechnics, explosive remnants of war, and terrorist training. The chapter highlights initiatives and strategies for restricting access to materials and knowledge and strengthening international cooperation and information sharing. It also emphasises the need to monitor and regulate the online space, where radicalisation and training often occur. Public-private partnerships and community engagement are crucial to identify and prevent potential threats before they materialise.

Research initiatives and collaboration

Several projects have addressed security challenges, including preventing concealed explosives, smuggling explosive remnants of war. The challenge to preventing the smuggling of explosive remnants of war (ERWs) lies in the inherent difficulty of detecting and intercepting these dangerous materials. Smugglers often use complex and innovative methods to conceal ERWs, making their detection challenging for security forces. Moreover, the vastness of international borders and the high volume of trade and travel increase the difficulty of thoroughly monitoring and inspecting all cargo and travellers.

The UNCOVER project seeks to enhance intelligence work to uncover attack plans involving concealed explosives. ANITA, ENTRANCE, and PARSEC focus on preventing the smuggling of explosives and improving checkpoint security.

Photo: FOI

PARSEC, in particular, aims to develop new technologies to detect illegal parcels in postal services.

The challenges of countering radicalisation and improving checkpoint security involve addressing complex factors and balancing effective prevention measures with minimal disruptions. Radicalisation prevention requires understanding of its root causes, identifying at-risk individuals, and combating the spread of extremist content online. That necessitates collaboration between governments, technology companies, and civil society organisations. The following projects have

focused on the topic of radicalization and improving checkpoint security.

To prevent radicalization, the PROHETS and CounteR projects have developed toolkits and platforms for reducing the number of individuals trained as terrorists. LAW-GAME uses gamification technologies to train police officers on effective experiential training and prediction of criminal actions.

UNCOVER also works on developing an efficient steganalysis framework to detect hidden information in digital media. ANITA targets online illegal trafficking by creating a user-centred investigation system. ENTRANCE aims to improve the non-intrusive inspection of cross-border freight movements through risk-based approaches. PARSEC focuses on parcel and letter security for postal and express courier flows by developing non-intrusive detection technologies.

Prohets and counter both aim to prevent future terrorist attacks by developing eu-wide security models and privacy-first situational awareness platforms, respectively, for data mining and prediction of critical areas.

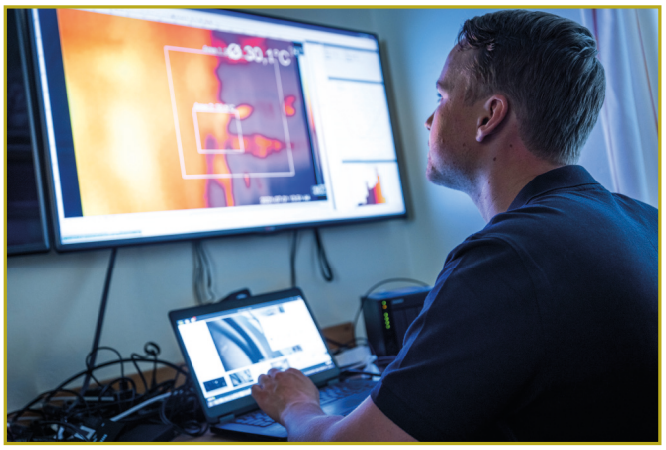


Photo: FOI

Examples of possible future initiatives:

- Limiting access to precursor materials for 3D printing IEDs and considering the need to register purchases of 3D printers.
- Collaboration with counter-narcotic forces to exchange experiences and applied methods.
- Financial support to incentivise people to hand in explosive remnants of war.
- Surveillance of foreign territory fighters and training camps to prevent terrorist activity.

Detect

Detection efforts focus on identifying concealed explosives, pyrotechnic-based IEDs, remnants of war, and individuals who have received terrorist training. The chapter emphasises developing and implementing advanced detection technologies and methodologies to identify various threats accurately. These include sensors and systems capable of detecting concealed and disguised explosives and monitoring and analysing online activity to identify potential terrorist training or radicalisation. Cross-border collaboration, data sharing, and integrating detection technologies within the security infrastructure are crucial for effective threat detection.

Research Initiatives

Not all detection technologies are equally suited for all scenarios; some require training, well-developed and exercised SOPs, and mechanical and logistic support. For some of the selected scenarios, cost-effective measures can be widely and easily implemented.

At European level, there are several research initiatives where the developed tools could potentially be applied; for example, MiRTLE is a low-cost threat detection system by Radio Physics Solutions that can detect concealed weapons and explosives up to fifty metres away. CONSORTIS aims to develop a stand-off concealed object detection demonstrator using a dual-frequency submillimetre-wave video camera and active 3D imaging radar system. TERASCREEN seeks to create a security screening technology for border checks using passive and active operation at several Terahertz frequencies. VMEWI3 aims to develop a technology demonstrator using remotely operated unmanned ground vehicles to detect indirect indicators of IED presence. MUSICODE will develop new unmanned ground vehicle stand-off capabilities to detect IED components. CONFIDENT aims to develop technology demonstrators using remotely operated platforms to confirm and identify IED components and provide complementary early warning capability. MKD proposes a new system of landmine detection based on unmanned aerial vehicles. COSMIC proposes a three-stage detection system with eight CBRNE sensors to detect CBRNE materials hidden in shipping containers and vehicles.

Photo: FOI

Exploration and development of new technology

A crucial factor for new detection technology is its ability to adapt to ever-changing attack methods rapidly. Suggested actions include standardised validation for their intended use, assessing cost-effectiveness, establishing EU-wide standardisation to address user needs better, and facilitating shared access to data sets at the EU level.

Collaboration

Successful innovation in the security industry relies on more than government initiatives like public funding or legislation. A promising future necessitates active involvement, commitment, and partnership from potential clients in the security sector, as well as proactive collaboration between various stakeholders, such as governments, regulators, policymakers, industry, innovators, research teams, and users. This collaboration accelerates innovation and ensures the efficient integration of innovative solutions into the security landscape.

Technologies suggested for further development:

- Continuous technology updates and personnel education to detect emerging threats is needed.
- Concepts to detect pyrotechnic materials and bomb-making factories are essential.
- Improved intelligence and detection methods to disrupt smuggling activities should be applied.
- Biometric identification and centralised databases to spot suspicious individuals and patterns are considered valuable.

Mitigate

In the described circumstances, the possibilities to mitigate the effect of explosives are independent of the underlying motivation of a perpetrator. Here, we highlight the importance of protecting existing infrastructure and striving for it during planning and construction. Quantitative risk analysis is one tool that can guide the decision process by balancing costs and effectiveness.

Research areas

Structural and design measures that mitigate explosion effects are available and have been investigated in various research projects. The specific applicability of each action depends on the location of interest, and a cost-benefit analysis should be conducted. During the design phase of places or buildings, fundamental mitigation aspects, such as safeguarding the distance between the target and potential attack, can be considered. Hazards from fragmentation can be reduced using blast-resistant components and appropriate separation of places. Organisational measures that can minimise explosion effects include reducing people's exposure, evacuating people, and training first responders. First responders do not know what kind of explosive might be inside the IED. Instead, the response to an attack depends on the location and surroundings of the IED.

Research initiatives

Physical and organisational mitigation measures for EU civil security depend on the location and surroundings of IEDs rather than the type of IED. Research projects such as AURIS, ELASSTIC, SPIRIT, SUSQRA, and TACTICS have developed tools, technologies, and methods to enhance security, reduce damage, and improve attack response. AURIS established a security management system for critical infrastructure and building health monitoring. ELASSTIC focused on building design and sensor technology. SPIRIT developed tools to enhance the security of large buildings against terrorist threats.

Photo: FOI

SUSQRA aimed to create software for post-blast IED damage evaluation. TACTICS developed tools for improving security forces' ability to prevent and handle urban attacks.

Further Research

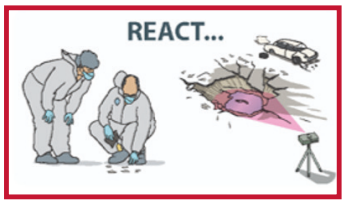
Consequently, a field for further research could be identifying simple and cheap technological and organisational measures to mitigate explosion effects, whenever this always has to go hand in hand with the prevent- and detect measures. The basis could be quantitative risk analysis, where different kinds of measures, their costs, and their effectivity are evaluated against each other.

Photo: FOI

Suggested measures include:

- Infrastructure known as a target for attacks can be put where their destruction limits collateral damage.
- Organisational measures that can minimise explosion effects include reducing people's exposure, evacuating people, and training first responders.
- Making existing solutions available and research results easily accessible to end users

React



The React domain in Year 5 focuses on emergency management and response in the context of concealed explosives, pyrotechnic-based IEDs, explosive remnants of war, and terrorist training. The chapter discusses the importance of swift and effective incident response, including interagency coordination and communication. It also emphasises the need for advanced training and resources for first responders, law enforcement, and medical personnel to minimise casualties and ensure the safety of affected individuals. Lastly, the chapter highlights the significance of post-incident investigations, analysis, and information sharing to improve future prevention, detection, and mitigation efforts.

To REACT to the terrorist attack timeline requires improved collaboration and communication between European forensic and research institutes and first responders, police, law enforcement, and the judiciary. Projects such as ACRIMAS, AUGGMED, CAST, XClanLab, RISEN, ROSFEN, BRIDGE, DARIUS, DirtyBomb, GIFT-CBRN, and PRACTICE aim to facilitate this cooperation by providing training for coordinated and rapid response to attack scenarios, enabling first responders to assess a crisis without endangering themselves, developing solutions for stable and uniform crisis management, and exchanging expertise regarding new solutions necessary to civil security. These projects also prepare for realistic threats, for example, dirty bombs, attacks on critical infrastructure, and remote-operated vehicle attacks.

Challenges & possibilities in React

There are still many challenges to overcome with respect to combating and reacting to the chosen scenarios. Improved and more extensive monitoring and surveillance of the trafficking of illicit material on the darknet, could reduce the number of attacks. In addition, the surveillance of social media could be intensified.

Photo: FOI

Research on organizational measures is suggested regarding:

- Improvement of post-blast investigation concerning forensics, but also information sharing are suggested.
- Combination of efforts is likely beneficial to follow and anticipate developments in the scene.
- Tracing the origin of used explosives and other components.
- EODs should prepare for emerging threats, and publishing HME synthesis should be limited in scientific literature.

Forensic investigation. Photo: FOI

Surveillance of social media. Photo: FOI

Concluding remarks

Our research has identified a range of innovative technologies, procedures, and strategies that hold the potential to enhance public safety across the four counter-attack domains significantly: Prevent, Detect, Mitigate, and React. We rigorously evaluated these options in light of the annual scenarios considered.

In the Prevent domain, initiatives aim to identify and track potential threats. In contrast, the Detect domain highlighted advances in surveillance and stand-off detection techniques. The Mitigate domain focused on addressing challenges in soft targets and infrastructure protection. The React domain emphasised the importance of forensic analysis and improved communication between actors.

It is essential to consider the context of any project deployment and the potential consequences on individual freedom, higher costs, and societal disruption. Striking the right balance between security and potential negative societal impacts is crucial. Proposed solutions must be assessed for their effects on individual rights and freedoms, as well as their financial viability and sustainability.

In conclusion, our study has revealed significant findings with the potential to contribute to developing more effective public safety strategies across the four counter-attack domains. Policymakers and practitioners must acknowledge that these initiatives require careful evaluation and tailoring to meet community needs and conditions. We hope our work will be a foundation for further research and discussion in this critical area.

Please visit our EXERTER's web-page, or contact us for more information about our work and activities.

EXERTER CONSORTIUM

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.