30/11/2020

Version no. 1.0

Security of Explosives pan-European Specialists Network

D6.5
EXERTER 5th report on innovations, standardisation and exploitation within SoE

FOI
FhG-EMI
BKA
ENEA

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

D6.5
EXERTER 5th report on innovations, standardisation and exploitation within SoE

Main Author(s) - (Public)	
Name	*Organisation*
Matilda Ågren	FOI
Contributors	
Main Author(s) – Annex 1 **(Unclassified - Consortium confidential)**	
Name	*Organisation*
Matilda Ågren	FOI
Contributors	
Ola Norberg	FOI
Emma Lundell	FOI
Johannes Schneider	FhG-EMI
Roberto Chirico	ENEA
Main Author(s) – Annex 2: Scenario 3 - Preliminary requirements list **(EU-Restricted)**	
Name	*Organisation*
Johannes Schneider	FhG-EMI
Roberto Chirico	ENEA
Matilda Ågren	FOI
Contributors	
Main Author(s) – Annex 3: Scenario: Public transport - The second annual summary in EXERTER (Public)	
Name	*Organisation*
Emma Lundell	FOI
Roberto Chirico	ENEA
Johannes Schneider	FhG-EMI
Rasmus Schulte-Ladbeck	BKA
Matilda Ågren	FOI
Contributors	

Document information	
Version no.	*Date*
1.0	30/11/2020

Summary

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

The D6.5 deliverable concludes the work on the 2nd yearly scenario, an attack in the public transportation system, based on the Madrid train bombings on March 11th 2004, and addresses findings related to the annual EXERTER Conference. It also introduces the 3rd EXERTER scenario, a person borne IED attack, and provides the preliminary associated user requirements short list.

Three annexes are connected to this report: Annex 1, which is the consortium confidential version of the D6.5 report, available to all in the EXERTER consortium and all members of the EEC; Annex 2 that is a security classified EU-Restricted annex containing the preliminary requirements for the year 3 scenario; and Annex 3 providing a public and accessible summary of analysis and recommendations for the year 2 scenario.

Contents

1 Introduction

1.1 Background

EXERTER connects 21 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 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.

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 different counter attack domains are continuously pursued for 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, and have, to large extent, different sets of users and stakeholders, thus setting a wide scope for the EXERTER network.

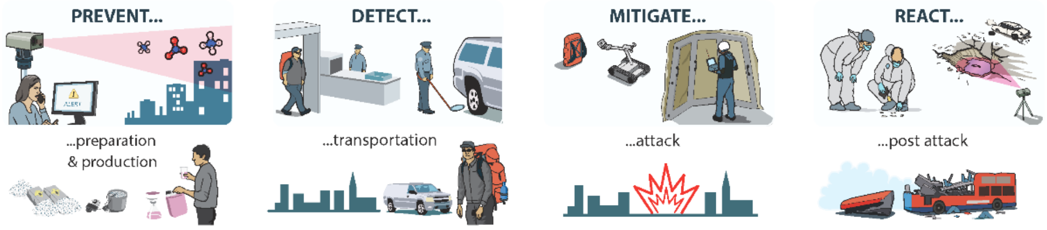

Figure 1: The counter attack domains addressed by EXERTER.

1.2 Objectives and content of the report

This report is the fifth of the 6-monthly Deliverables on analysis and recommendations in the EXERTER project. It consists of one main report and three annexes.

In Annex 1, highlights from the year two scenario, an attack in the public transportation system based on the March 11th 2004 Madrid train bombings, is presented. This scenario and its specific key elements, connected to each counter attack domain, were described in deliverable D6.3 - *EXERTER 3rd report on innovations, standardisation and exploitation within SoE*, and analyses and recommendations connected to the scenario were presented in deliverable D6.4 - *EXERTER 4th report on innovations, standardisation and exploitation within SoE*.

Annex 1 also introduces the year three scenario, a person borne IED attack, and provides the associated preliminary end user requirements short list. This scenario has been discussed during national discussions that this year replaced the practitioner workshop due to the ongoing pandemic. The scenario and the support for the national workshops is presented in Annex 1. A preliminary list of requirements and needs is provided in the EU-Restricted annex, Annex 2.

Annex 3 is the second annual summary in EXERTER, covering the analysis and recommendations for the 2nd EXERTER scenario, the public transportation attack.

The person borne IED attack scenario will be further explored in the next two 6-monthly reports on innovations, standardisation and exploitation within SoE, D6.6 and D6.7. The requirements and gaps related will be further analysed, and recommendations connected to research initiatives, standardisation and certification opportunities and exploitation support will be provided.

2 Concluding remarks

The EXERTER network has been put in place in order to enhance society’s capability to fight terrorism and serious crime related to the use of explosives. To this effect, EXERTER puts special emphasis on the four terrorist attack countermeasure domains PREVENT, DETECT, MITIGATE and REACT and pursuing the identification of the best ways forward in terms of research initiatives, standardisation and certification, and exploitation opportunities.

The D6.5 deliverable reports on the 2nd year scenario, focusing on new findings as a result of the 2nd EXERTER conference, and introduces the 3rd year scenario - providing the associated preliminary practitioners’ requirements short list. Emerging explosive threats, possible variations and alterations of the second yearly scenario is included in the scenario definition, providing EXERTER with a relevant and up to date scenario.

Due to the pandemic, it has been necessary to make adaptions both of the EXERTER conference and the practitioner workshop. The conference was held as a virtual event, which was both highly appreciated and well attended. The workshop on the other hand is replaced by discussions on a national and/or organisational level since requirements in general is to be security sensitive, and thus cannot be communicated via an online platform.

The person borne IED attack scenario will be further addressed in detail in the upcoming 6-monthly deliverables, D6.6 and D6.7.

3 Abbreviations and Definitions

CI	Classified Information – notation referring to information security classification
CO	Consortium Confidential – notation referring to information dissemination level
D	Deliverable
EC	European Commission
EEC	End user and Expert Community, external group of stakeholders in the field of SoE which have agreed to support and interact with the EXERTER consortium
IED	Improvised Explosive Device
LEA	Law Enforcement Agency
M	Month since project start
R&D	Research and Development
SoE	Security of Explosives

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.