21/10/2019

Version no. 1.0

Security of Explosives pan-European Specialists Network

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

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

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

PUBLIC

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

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

Document information	
Version no.	*Date*
v. 1.0	21/10/2019

Executive summary

Introduction and background

The report D6.2 is the second of the 6-monthly Deliverables on analysis and recommendations in the EXERTER project. It aims at summarising information on innovations, standardisation and exploitation based on the findings in the project related to a yearly scenario. This year's scenario was the July 22nd 2011 bombing in Oslo, Norway.

EXERTER is a H2020 project that connects 21 practitioners from 13 EU Member States (MS) and associated countries across Europe into a Network of Explosives Specialists. The network aims at identifying and promoting innovative methodologies, tools and technologies that will offer solutions in the fight against terrorism and serious crime, i.e. enhancing the overall Security of Explosives. The core of the EXERTER network brings together experts coming from Law Enforcement Agencies (LEA) and Military Institutes, Governmental and Civilian Research Institutes, Academia and Standards Organisations.

A yearly scenario is 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.

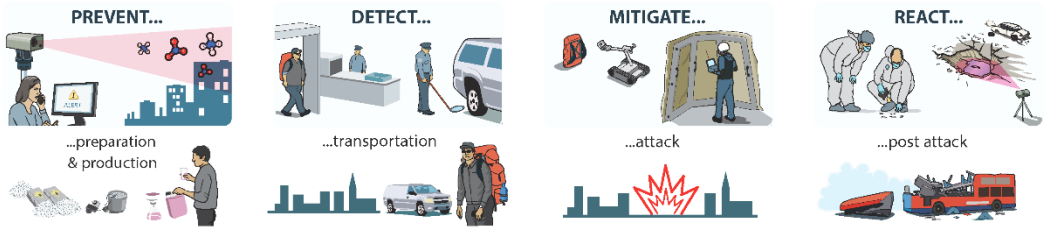

Figure 1: The counter attack domains addressed by EXERTER.

In the report, identified requirements and gaps connected to the yearly scenario are described, as well as the efforts made to assess a research review, standardisation and certification priorities, and exploitation support. Analysis and recommendations related to the yearly scenario for the different counter attack domains concludes the report and points towards research needs and proposed focus areas.

Identified requirements and gaps

Some identified requirements and gaps are presented in the report. These are based on analysis of input received from stakeholders and the expert community. The requirements and gaps are connected to security of explosives capabilities. The report also highlights some areas that are believed to be the most important to work with within the respective counter attack domain.

Research review

In a research review, information from national, European, and international research projects related to Security of Explosives (SoE) that can help in the fight against terrorism, are identified and collected. Both ongoing and completed projects are considered. Projects are continuously assessed through literature surveys, interaction and communication with other research projects, web searches and interviews.

The most auspicious research activities, which can counter existing practitioner needs and gaps, are highlighted and further studied. Related to the yearly scenario, the highlighted projects for the counter attack domain prevent were BONAS, EMPHASIS, ERNCIP, EXPEDIA, LOTUS and PREVAIL. For the detect domain C-BOARD, EFFISEC, EUROSKY, IMSK and EDEN were considered relevant, and for mitigate ELASSTIC, SPIRIT, VITRUV, ENCOUNTER, TACTICS, AVERT, EDEN and SUBCOP

were deemed especially interesting. For the react domain ACRIMAS, BRIDGE, E-SPONDER, SAVASA, FORLAB, HYERION, ROSFEN and SUSQRA are relevant.

Standardisation and certification priorities

Standardisation, certification and regulation affects the possibilities for innovations to reach the market and it can contribute to filling the identified capability gaps. Through interactions with practitioners, private sector and standardization bodies an assessment of standards relevant for the EXERTER project has been assessed and connected to the different counter attack domains.

Standardisation entities of particular interest are for example "CEN/TC 391 Societal and Citizen Security and ISO/TC 292 Security and resilience", and for the yearly scenario (Oslo, 2011), specifically "CEN/TC 160 Fertilizers and liming materials".

In the prevention domain the EU regulation on the marketing and use of explosives precursors, EU Regulation 98/2013, is central. It regulates the availability and allowance to possess certain chemicals, e.g. ammonium nitrate, for the general public. An update of the regulation is underway. Related to the counter attack domain detect it is pointed out that existing guidelines and standards are focused on the aviation security and customs areas for detection of explosives. It is also noted that some procedures for vehicle screening exist. Connected to mitigation the manual "Reference Manual to Mitigate Potential Terrorist Attacks against Buildings FEMA-426/BIPS-06/October 2011", which is a part of the new Building Infrastructure Protection Series published by the United States (U.S.) Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Infrastructure Protection and Disaster Management Division (IDD), is highlighted. It serves to advance high performance and integrated design for buildings and infrastructure.

Exploitation support

Technology and tools are central in countering the terror threat and bridging the gaps and requirements. Thus, EXERTER works with finding appropriate state-of-the-art technology in the field of SoE, and focuses on supporting collaboration and interaction between different actors to improve exploitation possibilities. The latter could be achieved through creating a link between academia, industry, researchers and end users.

A generic overview of state-of-the-art technologies has been compiled. To support collaboration and exploitation the European industrial market is screened to find companies that could be useful and add value to the EXERTER project. The possibility to include them in the EEC, End user and Expert Community, or to engage with them in other ways, e.g. consultations or other networking activities, is then evaluated. The main purpose is to cover a wide range of counter tool technologies, avoiding overlaps between them in different fields of knowledge.

Analysis and recommendations

Prevent

The analysis of the counter attack domain prevent has been classified EU confidential and is not included here.

Detect

The analysis of the detect domain focuses on the detection of VBIEDs (vehicle borne IEDs) and of ammonium nitrate based HMEs (Home Made Explosives).

For vehicle screening, there is lack of suitable detection equipment. Research into new detection technologies and novel ways of using existing technologies and combinations of technologies, perhaps from other fields, could possibly bridge this gap. At European level, there are several research initiatives whose results potentially could be applied for vehicle screening. Partially applicable to the Oslo scenario are for example C-BOARD, EFFISEC and IMSK.

Screening processes could for example include stand-off detection of trace contamination, vapour detection technologies and techniques for detecting concealed explosives whilst the driver and

passengers are still in the vehicle. It is noted that vehicle screening poses some specific challenges, which can be translated to requirements on the technology used.

Some of the gaps that have been identified are for example training of personnel, automatic license plate and vehicle security cameras, new methods to identify suspicious behaviours (people, vehicles), driver identification with facial recognition with CCTV system, stand-off detectors (traces, bulk, anomalies, non-chemical components, etc.).

Mitigate

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

Past research initiatives that address aspects of improving mitigation of explosion effects are example SPIRIT and ELASSTIC, which aimed at improving the physical security of large buildings. Others are ENCOUNTER that focused on the neutralization of IEDs, SUBCOP that proposed a shield type configuration to isolate suicide bombers in order to minimise the effects of an explosion, and AVERT that added another point of view by describing methodologies to remove the potential threat source from the scene. Two exemplary projects researching on organizational measures were TACTIS or EDEN that aimed at improving the effectiveness of security forces and at enabling them in a proper situational assessment.

For mitigating explosion effects some potential solutions already exist. For example, barriers or bollards surrounding the building to be protected and an appropriate landscape design can increase stand-off zones, which is one of the most important mitigation measures to reduce blast effects. However, it is noted that the implementation of stand-off zones has to be combined with an appropriate access control and checkpoints, and that organisational measures, such as emergency- and evacuation plans or even the neutralization of the (VB)IED, also can mitigate the effects from the explosion.

Mitigating the explosion effects by using physical security measures is a part of building design, and implementing measures while still remaining the building's functionality, openness and affordability can be central. In order to balance out the security/protection level with other targets (as costs, architectural parameters, environment, and office spaces), structural vulnerability assessments as well as an iterative risk management approach is strongly recommended. Consequently, initiatives aimed at developing procedural standards (e.g. quantitative risk analysis in the design process of critical infrastructure), design guidelines and certification of protection standards are needed.

Some other possibilities for future research that are pointed out in the report are e.g. developing mobile structural components to reduce blast effects, process to integrate physical security assessments into the common design process, making existing solutions available to the end user community and basic research on physical security aspects of new façade components and load bearing.

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

React

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

Since different national regulations and responsibilities come into effect in different countries, applicable standardisation, which comes into place in the aftermath of an extensive emergency, is scarce.

Nevertheless, several research projects deal with the topic of crisis management but it is unclear to what extent these research efforts can be, or are being, transferred into standard operating procedures and the practical work.

A considerable amount of research appears to be conducted in the area of stand-off detection of hazardous substances in the context of forensic analysis. The implementation of these techniques into best practice manuals or standardised procedures have not been observed, possibly due to the lack of commercially available systems.

Future work

A preliminary selection of projects that are of special interest for EXERTER have been finalised, and a selection of them have been highlighted as of special interest in relation to the first yearly scenario. Information on research activities, which can play a role in the identified gaps, will be further lifted for discussion, and considered as topics for the next annual workshop.

Regarding standardisation and certification, the efforts until now have mainly been focused on identifying standardisation entities related to EXERTER in general, and to establish connections with these entities. Central for the future work is to extend the review to better cover certification and regulations, and to identify and analyse gaps in current standardisations and certifications in relation to the yearly scenario, and to find opportunities for bridging these gaps.

An initial inventory of technologies that could prevent, detect, mitigate and/or react to a terror attack have been set up. Taking into account the current knowledge and experience, it is also planned to include more companies dedicated to each of the counter attack domains in EXERTER and to study different types of technologies that are currently developed which might have the possibility to be used within the counter attack domains. Work on identifying methods to facilitate the transfer of knowledge from universities to companies will be continued, and consultations will be set up.

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