05/12/2019

Version no. 1.0

Security of Explosives pan-European Specialists Network

D6.3
EXERTER 3rd report on innovations, standardisation and exploitation within SoE

FOI
KEMEA
BKA

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

D6.3
EXERTER 3rd report on innovations, standardisation and exploitation within SoE

Main Author(s)	
Name	*Organisation*
Matilda Agren	FOI
Ioannis Daniilidis	KEMEA
Erik Plessinger	BKA
Rasmus Schulte-Ladbeck	BKA
Ola Norberg	FOI
Contributors	
Patrik Krumlinde	FOI
Roberto Chirico	ENEA
Anneli Ehlerding	FOI
Main Author(s) – Annex 1 (Consortium confidential)	
Name	*Organisation*
Matilda Ågren	FOI
Ola Norberg	FOI
Contributors	
Rasmus Schulte-Ladbeck	BKA
Erik Plessinger	BKA
Anneli Ehlerding	FOI
Main Author(s) – Annex 2 (EU-Restricted)	
Name	*Organisation*
Matilda Ågren	FOI
Ioannis Daniilidis	KEMEA
Contributors	
Christian Ulrich	FhG-ICT
Frank Schnürer	FhG-ICT
Lara Hettmanczyk	FhG-ICT

Document information	
Version no.	*Date*
1.0	05/12/2019

Summary

This document is the third 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 D6.3 deliverable reports on the 1st yearly scenario, based on the July 22nd 2011 bombing in Oslo, Norway, focusing on new findings and feedback received as a result of the 1st annual stakeholder workshop. It also introduces the next annual scenario, which is a public transport scenario based on the March 11th 2004 Madid bombing, and provides the associated user requirements short list and describes possible alterations of the scenario and emerging threats.

Two annexes are connected to this report, Annex 1 and Annex 2. In the consortium confidential annex, Annex 1, the full versions of Section 2 and Section 3 (Section 3.5 excluded) in this report are presented. Annex 1 is available to all in the EXERTER consortium and all members of the EEC. In Annex 2, which is security classified EU-Restricted, all information regarding requirements (Section 3.5) and emerging threats (Section 4.2) is presented.

Contents

1 Introduction

1.1 Background

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

The main objectives of EXERTER are:

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

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

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

1.2 Objectives, content of the report and delimitations

This report is the third of the 6-monthly Deliverables on analysis and recommendations in the EXERTER project. It aims at presenting new findings, highlights and recommendations from the 1st annual stakeholder workshop covering the first yearly scenario, the July 22nd 2011 bombing in Oslo, Norway, and introducing the second yearly scenario, based on the March 11th 2004 Madrid bombing. The preliminary user requirements short list associated with the second yearly scenario and variations of the scenario, discussed during the second annual practitioners' workshop, is provided in the EU-Restricted annex, Annex 2, to this report. Information limited to the consortium is placed in Annex 1.

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.

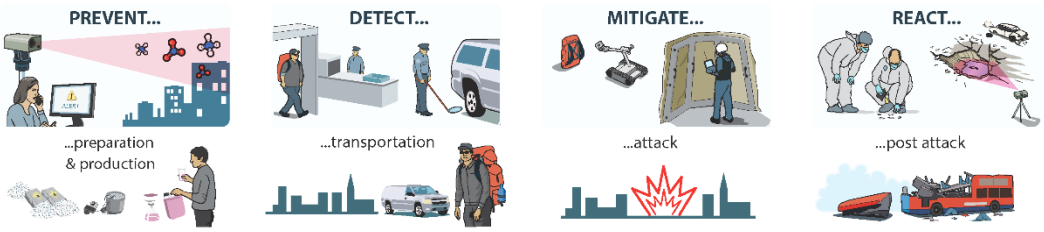

Figure 1: The counter attack domains addressed by EXERTER.

The Oslo scenario and its specific key elements, connected to each counter attack domain, were described in the EU-restricted D6.1 Annex 1, and analyses and recommendations connected to the scenario were presented in D6.2 with annexes.

The second yearly scenario, based on the Madrid train bombings, will be further explored in the following 6-monthly reports D6.4 and D6.5 where requirements and gaps related to this scenario will be further analysed and recommendations connected to research initiatives, standardisation and certification opportunities, exploitation support will be provided.

2 Content and highlights from the 1st annual stakeholder workshop

The EXERTER annual Stakeholder workshop, held in Oslo in April 2019, covered the explosive attack on 22 July 2011 in Oslo, Norway. The scenario is described in D6.2 - *EXERTER 2nd report on innovations, standardisation and exploitation within SoE,* and in the annex to D6.1 - *EXERTER 1st report on innovations, standardisation and exploitation within SoE.*

Parts of the information in this section has been considered consortium confidential and is thus only available in the consortium confidential annex to this report, Annex 1. The annex is available to everyone in the EXERTER consortium and members of the EEC.

2.1 Presentations, interaction forums and discussions

An introduction to EXERTER and to the Oslo Scenario opened the workshop and it then followed sessions with presentations related to each of the counter attack domains. A visit to the 22 July Information Centre in Oslo concluded the first day of the workshop.

2.1.1 The Oslo attack - key activities

The attack is presented in chronological order and the audience is given an overview of everything from the perpetrator's childhood to the trials and his court verdict. Recordings from the CCTV showing the execution of the attack is shown. A detailed description of the scenario can also be found in EXERTER deliverable D6.1 Annex 1.

2.1.2 Prevent

PREVENT session:	
Prevent aspects in the EXERTER project	FOI
XClanLab	Patrik Krumlinde, FOI
Regulation on precursors	DSB
Precursor monitoring	Christian Sørensen, KRIPOS

2.1.2.1 Prevent aspects in the EXERTER project

Some of the key aspects of the Oslo scenario given in the overview for the Prevent domain were:

- A business was established for making purchases of chemicals
- Precursors were bought online
- The bomb was constructed in a remote rural location

It has been studied if and how the currently implemented EU regulation on precursors (98/2013) would have affected the 22nd July bombing in Oslo. Effects of any upcoming amendments to the regulation have not been analysed.

2.1.2.2 XClanlab

In the prevent session the project "XClanlab" was presented. XClanLab is a project that further develops a mobile application that was developed as a prototype in the FP7 project EXPEDIA.

XClanlab is a mobile application to guide and support first responders in the identification of clandestine laboratories and in how to act in such a situation. It is also a tool to put the first responder in direct contact with the proper experts.

The XClanlab application would not have been efficient in the Oslo scenario as it unfolded. However, it could have had an impact on the scenario if the chain of events leading up to the attack had been different. For example, if any first responders, which in this context is LEA:s, ambulance personnel or firefighters, would have visited the farm and used XCLanLab as support they would probably have identified the it as a location of a clandestine laboratory. This could for example have occurred if a neighbour would have reacted to the fumes created during the HME production, if the perpetrator would have had an accident or if there would have been a fire on the farm. There are other, real examples of when support, like this app, could have been helpful for law enforcement agencies.

2.1.2.3 Regulation on precursors

The presentation covered the EU regulations regarding precursors, EU regulation 98/2013, and chemicals, EU regulation 552/2009 (REACH), along with their relation to the national regulations in Norway and their implementation. There is an update of EU reg. 98/2013 in progress (expected to be applied in December 2020) and there are indications that it will be similar to the national requirements in Norway.

The implementation of the precursor regulations in Norway, and how to enforce them, was presented. EU regulation 98/2013 Annex II relies on companies/sellers to report suspicious transactions. To create awareness there have been efforts to perform information campaigns for farmers, pharmacies and universities. There are possibilities to give penalties to businesses for not complying with the regulation, but at the time of the workshop the system is considered to be new, and thus a positive reinforcement is sought. Fines are possible, but currently not enforced.

2.1.2.4 Precursor monitoring

Kripos has the NCP, Norwegian national contact point, for suspicious transactions, theft and significant and unexplained loss of explosives. It renders an overview that helps in investigations/intelligence.

NCP has a tip-off service via internet, email and phone where all police services (national and other nations) can reach them. The process of how they work with tip-offs is described, and it is mentioned that the amount of tip-off in Norway is small, which means that all cases can be handled individually. In comparison, the UK have many thousands of tips every year and they have a data system that narrows down the information.

It is concluded that the current precursor regulation, EU-reg 98/2013, potentially could have hindered the Oslo bombing if some purchase was reported (aluminium powder, sulphuric acid), and if Breivik would have been looked into (personal situation, does he own a farm etc.). Even if the case would have been suspicious, it is required that the local police look into it, or investigate in time to stop the attack.

2.1.3 Detect

DETECT session:	
Detection aspects in the EXERTER project	ENEA
ENTRAP	Ola Norberg, FOI
Vapor detection	Marta Jezierska- Switala, TNO

2.1.3.1 Detect aspects in the EXERTER project

Introduction to DETECT domain was given by a representative from ENEA. In the context of the Oslo scenario possibilities in the detect domain for example include; identification of the driver, identification the vehicle via its licence plate, and automatic identification of suspicious behaviour. Screening processes to find explosive residues could include equipment for detection of trace or bulk amounts of explosives, different techniques are available and suitable for different sets of requirements. Detection of vapours of explosive substances is also a possibility. Procedures for vehicle screening by customs and military were noted as interesting.

2.1.3.2 Presentation of ENTRAP project

The H2020 project ENTRAP, Enhanced neutralization of explosives threats across the plot, was presented by a representative from FOI. The project focuses on methods to assess tools that could counter explosive threats. Threat analysis and scenario descriptions are performed. Operational research methods are used to assess the counter tools' effectiveness, cost assessments, gap analysis, ethical assessments and societal compliance, recommendations for future research. The project started in May 2017 to and ends May 2020.

2.1.3.3 Vapour detection

A TNO representative presented a project at TNO focusing on detection of explosives in vapour phase. Instruments for vapour detection could for example be used for cargo screening and checking of unknown objects, as well as detection of bomb factories, people carrying explosives, and in post-attack situations. Vapour detection instruments could potentially be used for VBIED detection in the future.

To generate samples for vapour detectors, methods to achieve reproducible generation and quantification of vapours of explosives have been developed. A selection of substances are currently investigated.

What vapours that in reality will be present in a headspace is a central question. This depends on a number of parameters and studied are for example the relation between explosive material (mass and morphology), soak time, confined volume and confinement material. Some materials can act as a sponge on the vapours.

2.1.4 Mitigate

Mitigate session:	
Mitigation aspects in the EXERTER project	FhG-EMI
Building blast protection	Solveig Heggelund, NDEA

2.1.4.1 Mitigation aspects in the EXERTER project

A representative from Fraunhofer EMI gave an introduction to the MTIGATION domain. In the context of the Oslo scenario, four main aspects can be considered from a mitigation perspective; the creation of standoff distance in an urban and publicly available area, the building design and its blast resistance, the urban layout that can create pressure reflection effects, and organisational measures including neutralisation of the device and evacuation plans.

2.1.4.2 Blast protection of buildings

A representative from the Norwegian Defence Estates Agency held a presentation on the structural response of the buildings, estimation of the size of the charge used by Breivik and the security of the new governmental headquarters.

2.1.5 React

React session:	
React aspects in the EXERTER project	BKA
Presentations of post-blast investigation following the attack	Eva Ragde, Oslo Police District

2.1.5.1 React aspects in the EXERTER project

A representative from BKA presented aspects in the REACT domain. REACT covers emergency management, and in the context of the Oslo scenario topics such as interaction between organisations, risk minimisation for first responders, Crime Scene Investigation and forensics and collecting the intelligence necessary for immediate response – *manhunt* –, are highlighted.

2.1.5.2 Presentation of the post-blast investigations

A representative, who was responsible for the forensic investigation concerning the bombing, from the Oslo police presented the post-blast events of the July 22 attacks in Oslo.

The crime scene was described as special, and it posed several difficulties to the people working there. The workload was large, and the tasks included to investigate the site as well as to rig a headquarter, keep close control over searched areas, control all evidence/items and escort people visiting the site.

It is noted that there was no interaction with the EU during the investigation but that it would be favourable have more collaboration over the borders since the work procedures are comparable. The way the Oslo police works do not exclude the possibility for collaboration.

2.2 Analysis of the 1st annual stakeholder workshop

A more extensive analysis of the July 22nd Oslo scenario is covered in D6.2 with annexes. The analysis below is focused on the findings at the stakeholder workshop in Oslo 2019.

In the PREVENT session regulatory means to control the access to explosive precursors was discussed; the EU regulation 98/2013, the legislation implemented in Norway and their national work with enforcement. An update of the EU regulation is underway, and analysis of the new regulation will be performed when it is completed. Legislation based on the EU regulation is considered not to have the possibility to prevent all attacks with HME from taking place, but it does make it more difficult to produce HME, and the probability to be flagged and then caught when acquiring chemicals increases. Part of the regulation relies on the reporting of suspicious activities, where enforcement and implementation of automatic procedures for "flagging" is important. Education, information and implementation of procedures for businesses handling precursors and for smaller stores selling chemicals listed in EU regulation 98/2013 Annex II is highlighted as important. Having a central body to handle reported purchases and suspicious activity can provide a full image of the situation and be basis for investigation.

Technical support to first responders to identify clandestine laboratories is one possibility to prevent attacks. This can be provided by the mobile application XClanlab, which is under development.

Research initiatives and the possibilities of inhibitors for explosives precursors were not discussed.

Detecting fumes from bomb making facilities and vapours from the bomb could be possible via vapour detectors. A research initiative regarding vapour detectors for explosives and experimental methods for achieving reproducible results was presented. Many explosives have low vapour pressures, meaning that the concentration of vapour in the air around the explosive is low. Other techniques to detect and identify traces of explosives and precursors are available but generally require a screening process, or to be a part of a manual search.

CCTV with automatic systems for identification of the perpetrator, identification the vehicle via its licence plate and automatic identification of suspicious behaviour was not discussed during the workshop.

In the MITIGATION session, consequences of the attack, including effects from reflections of the shock wave, were discussed. Methods used to perform a reconstruction of the bomb were presented along with

aspects in the design of the new headquarter. The design process includes risk evaluations, and is e.g. combining efforts to achieve stand-off distance with enforcements for blast resistance.

After the attack, the situation at the crime scene was complex. The presentation in the REACT session covered how the risk for first responders and LEAs was balanced with the need to investigate and work on the scene. To quickly gain access to necessary resources posed a problem. A solution could potentially be increased cooperation over European borders in the case of extraordinary events that require a large number of specialists. For such collaborations to be efficient, work procedures should be harmonised across borders. The process of collecting forensic evidence was described.

Existing and emerging tools and methods to counter the explosives threat is assessed in the project ENTRAP, presented in the DETECT session. Information on different counter-tools and the methods developed to assess and evaluate them have the potential to be used in EXERTER.

3 2nd yearly scenario and preliminary requirements list

The second scenario that is used as basis for the work, workshops and discussions in EXERTER considers an attack on public transportation. The scenario is based on the 2004 Madrid train bombings, also known as "11-M"[1]. In order not to limit the discussions to a single past event, alternative scenario plots are also considered including possible emerging threat scenarios. The 2004 Madrid train bombing scenario is described in section 3.1 below. Based on the Madrid scenario, a generic scenario definition has been created, see section 3.2, and Highlights that could be studied further in EXERTER are presented in section 3.3. Variations of the scenario is discussed in section 3.4 and section 4.2 (see Annex 2 to this report).

A full version of this section is given in the consortium confidential annex, Annex 1 to this report. The annex is available to everyone in the EXERTER consortium and members of the EEC.

The scenario was presented at the practitioners workshop in Freiburg November, 19-20, 2019. Requirements and gaps were collected during the workshop. A preliminary list of requirements was collected based on the workshop discussions, see section 3.5 and Annex 2 to this report. An updated list will be compiled after this report is published and included in EXERTER D6.4.

3.1 Scenario description in brief

On the morning of March 11 2004, 10 bombs packed with nails and dynamite exploded on trains heading towards central Madrid. The blasts killed 191 people and injured approximately 1,800.

The ten IED exploded in four different trains, three more IEDs were found and neutralized by controlled detonation, and one IED was defused[2]. The bombs were contained in small bags.

The bombings were carried out by a group of young men, mostly from northern Africa, who were, according to prosecutors, inspired by a tract on an al-Qaida-affiliated website that called for attacks on Spain. The aim of the attack was to kill a large number of people to, in turn, provoke a reaction a few days before the Spanish general elections.

3.2 Generalised scenario context

The setting is a multiple and coordinated attacks on the public transportation system in a city. The time for the attack (morning with many commuters) is chosen to maximise the number of victims but also to be close to a political event (in the Madrid case an election) to affect the public opinion.

The perpetrators are organised in one or more cooperating terrorist cells.

For the IEDs, commercial explosives and detonators, triggered by mobile phone alarm functions, are used. The explosives and detonators are "purchased" via criminals who in turn either have bought it on the black market or stolen it. The IEDs are also equipped with e.g. nails and other metal objects aimed to function as shrapnel to maximise the effect.

3.3 Highlighted scenario aspects for further study within EXERTER

In this section, certain highlighted aspects of the attack are listed in respect to the different phases in the terrorist timeline.

[1] Wikipedia

[2] The total number of not detonated IED:s varies, depending on source, between 3-4

3.3.1 Prevent

- How to control the access to commercial explosives including detonators.
- The IEDs are assumed to be constructed and assembled at a location near the location of the attack, i.e. in a larger city.

3.3.2 Detect

- The multiple targets are commuter trains heading towards a large train station.
- The IEDs are "programmed" to detonate simultaneously at a large, central, train station.
- The time for the attack is chosen to maximise the result in terms of deaths and injured persons.
- The target area is public with no means of entrance security checkpoints.
- Rucksacks and bags are used to carry the IEDs
- The IEDs are based on commercial explosives, detonators and electronics.
- A large amount of shrapnel is applied.
- Security systems and equipment in place is CCTV operator.

3.3.3 Mitigate

- The target is crowded with people most of the time
- The target area is publicly accessible with no means of entrance security checkpoints
- The detonation takes place in a closed (train doors closed) or nearly closed (train doors open) small and crowded containment

3.3.4 React

- The first to arrive at the scene is the emergency services.
- The mobile phone network collapsed for several hours
- Search for secondary IEDs?
- Bomb squad/police vs rescue of injured people.
- Collection of evidence?

3.4 Alterations of the 2nd yearly scenario

The second yearly scenario is an attack that targets the public transportation system. The scenario uses the Madrid train bombing as base, but variations of the scenario is considered in order to be able to consider similar attacks that could be executed in the future. During the practitioners workshop the participants were asked to not limit the discussions to only cover the Madrid bombing but to also think of possible future attack scenarios. Some possible alterations of the attack is presented below.

The motivation for carrying out an attack on public transportation could vary. Some possibilities that potentially could drive motivation are i.e. MENA (Middle East and North Africa) conflicts, migration crisis, environment and globally interconnected crises. The Madrid attack had jihadist motives, but other extremist views, such as right wing extremism could be the driver for similar attacks in the future.

The perpetrators in the Madrid case was organised as a large cell, and were connected to/in a network. It should be considered that new on-line platforms provides different ways for individuals to radicalise and to plan and organise attacks. This could e.g. affect the size of the network and the speed to mobilise. It might make the need for physical meetings obsolete, and it could affect money transfer procedures and communication. Technology enablers such as computing and telecommunications introduce the additional dimension of digital and cyber to the landscape of the physical order.

The explosive devices were constructed of commercial explosives. The possibility to use various types of homemade explosives is a potential alteration, as well as the possibility to acquire commercial explosives abroad and transport them into another country to perform an attack.

The attack could potentially target other means of transports than commuter trains. Busses, high-speed long distance trains, ferries, subway trains or trams are alternative, but similar target options.

3.5 Preliminary requirements list

A preliminary list with requirements is provided in the EU Restricted Annex 2 to this report. The requirements were extracted from discussions during the annual practitioner workshop in Freiburg, 19-20 November, 2019.

4 Threats and attack strategies

In EXERTER, work is performed to identify the evolution of threats and attack strategies. This in order to draw conclusions on new trends and patterns of threat and attack strategies and to extrapolate these into possible predictions of future events. In this section, the findings until date are presented.

4.1 Trends/worldwide Europe

Terrorism incidents have been taking place across Europe for a long time. Terrorism in Europe has killed 11,288 people in 18,811 attacks since January 1970, according to the University of Maryland National Consortium for the Study of Terrorism and Responses to Terrorism's Global Terrorism Database, which tracks more than 170,000 foreign and domestic incidents worldwide [3].

In recent years, the terror attacks in Europe have been related to extremist groups with religious, political, and economical motives. Recruited and/or radicalized in an organised environment, the acts have been performed by groups or by individuals (lone actors). Attacks involving the use of Improvised Explosive Devices (IEDs) have during past years caused a large number of victims. In Europe, some examples are; the Madrid train bombing in 2004, the London bombings in 2005, the bombing of the Oslo governmental quarters in 2011, the Paris attacks in 2015, the Brussels bombings in 2016, and the Manchester arena bombing in 2017.

The availability of literature and other information media on the subject of preparation of Home-Made Explosives (HMEs) has created potential laboratories anywhere. An example is the series of incidents that occurred during 2015 and 2016 in France with terrorism-related deaths of more than 220.

4.2 Emerging threats

The explosive threat is continually evolving and changing. Driving factors are for example external circumstances that affects radicalisation, technological development and possibilities, and new implemented counter measures that drives adaptation. A selection of emerging threats is presented in Annex 2 to this report.

[3] https://www.start.umd.edu/gtd/

5 Conclusions and recommendations

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.

Every 6 months, EXERTER will issue Deliverables on Analysis and recommendations related to a yearly scenario. These Deliverables will entail the main findings across all WP's and will form the basis of the material that can be communicated to the wider SoE stakeholder community.

The D6.3 deliverable reports on the 1st yearly scenario, focusing on new findings and feedback received as a result of the 1st annual conference, and introduces the next scenario of the year and providing the associated user requirements short list. Emerging explosive threats, possible variations and alterations of the second yearly scenario is addressed in the report, providing EXERTER with a relevant and up to date scenario.

Presentations during the 1st annual conference were tightly connected to the Oslo scenario, and provided great insight into the attack and its consequences. Upcoming workshops and conferences will be more loosely connected to the yearly scenarios, taking a more general approach and allowing more focus to be placed on emerging threat scenarios. In addition, the workshops and conferences will put greater emphasis on discussions.

The March 11 bombing in Madrid in 2004 will be addressed in detail in the upcoming 6-monthly deliverables.

6 Abbreviations and Definitions

CAC	Counter-Attack Coordinator, an EXERTER project internal response domain expert who ensures a domain specific focus across WP implementation
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
ESETF	Explosives Security Experts Task Force
HME	Homemade Explosive
IED	Improvised Explosive Device
LEA	Law Enforcement Agency
M	Month since project start
MS	Member State
R&D	Research and Development
SoE	Security of Explosives
WP	Work Package

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