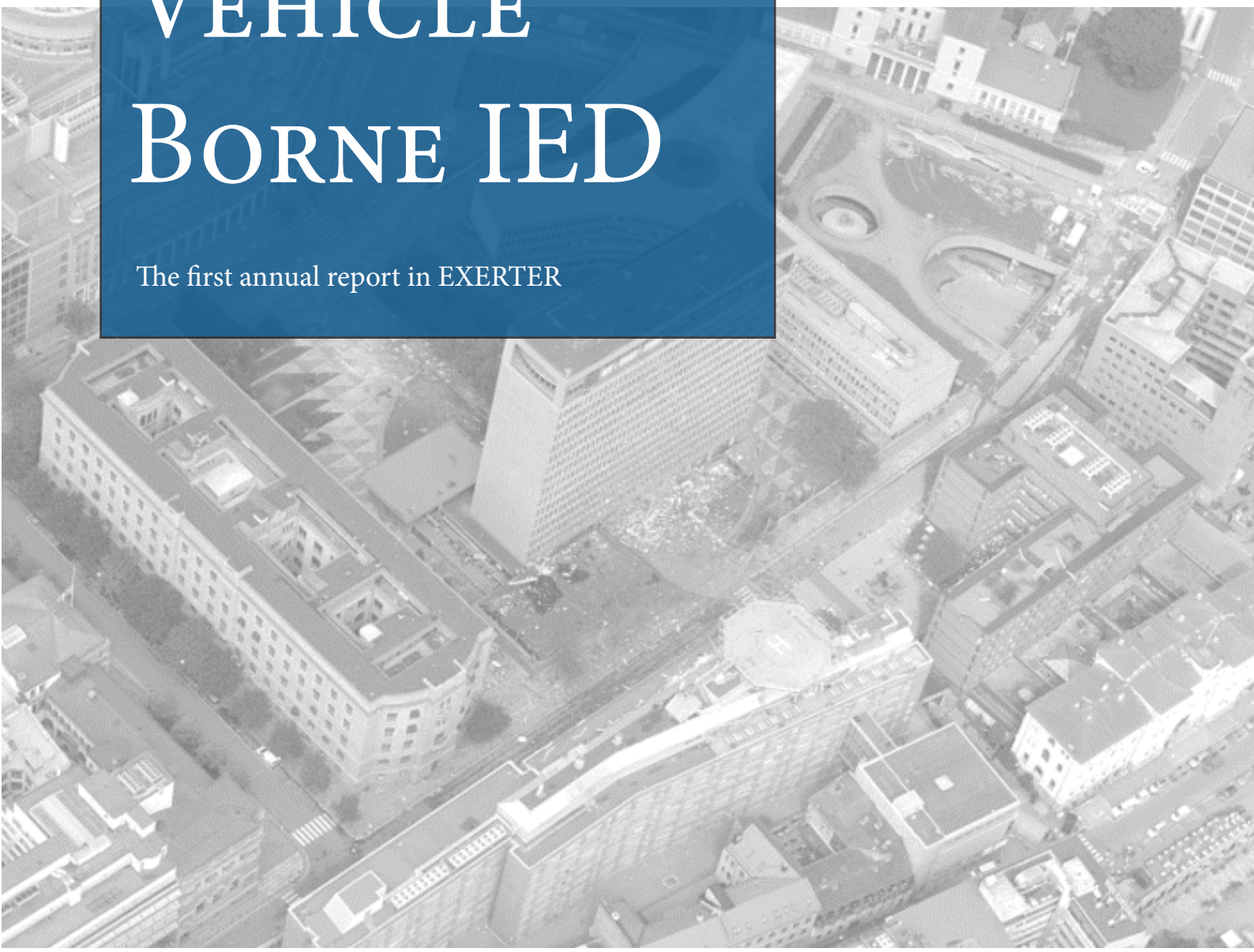
Scenario: Vehicle Borne IED

The first 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: Vehicle Borne IED -
The first annual report in EXERTER

FOI-S--6273--SE
FOI-2017-1045
September, 2020

Photo on front page: Regjeringskvartalet in Oslo.
Credit: Oslo policedistrict

Security of Explosives pan-European Specialists Network

EXERTER is a pan-European network that aims at identifying and promoting innovative methods, 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), Military Institutes, Governmental and Civilian Research Institutes, Academia and Standards Organisations.

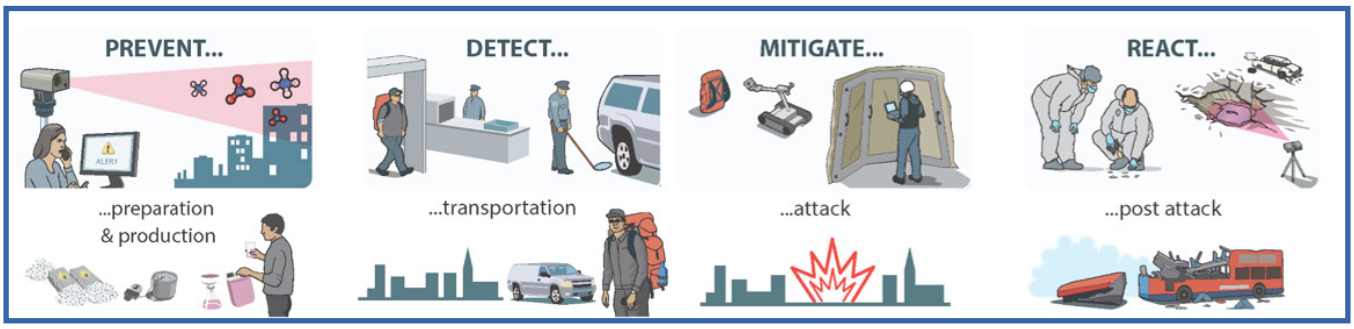
By enabling the exchange of information about the challenges of countering current and emerging terrorist threats, the related operational requirements on methodologies, tools and technology and the status in Research and Innovation, EXERTER will provide practitioners with the operative knowledge and tools for enhancing the security of our society.

Each year, EXERTER will focus on a scenario with connection to Security of Explosives. The scenario for the first year was based on the Oslo bombing in 2011, and some of the work related to it is presented in this report.

Information in this report is collected from the EXERTER reports D6.2 - 2nd Report on Innovations, Standardisation and Exploitation within SoE, v2.1, Mar 2020, and D6.3 - 3rd Report on Innovations, Standardisation and Exploitation within SoE, v1.0, Dec 2019

Introduction

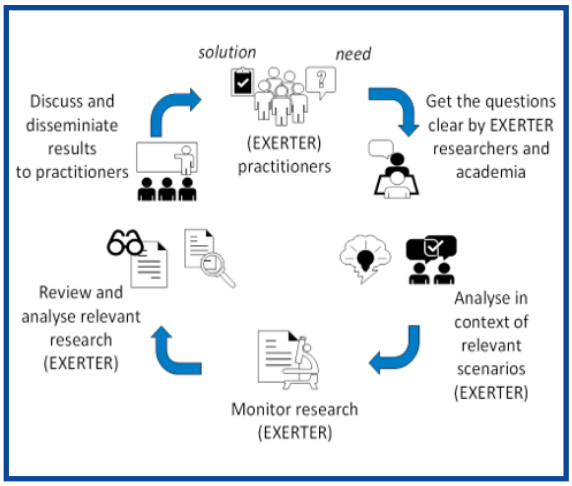
Each year, EXERTER defines a scenario, based on relevant input from practitioners and experts, and works with issues related to that scenario in all four phases on the time-line: PREVENT, DETECT, MITIGATE and REACT. EXERTER studies requirements, gaps and activities within research, standardisation and certification, and works towards exploitation of innovations within all phases.



Countermeasures under the four domains differ technically and operationally, and have different sets of users and stakeholders, thus setting a wide scope for the EXERTER network.

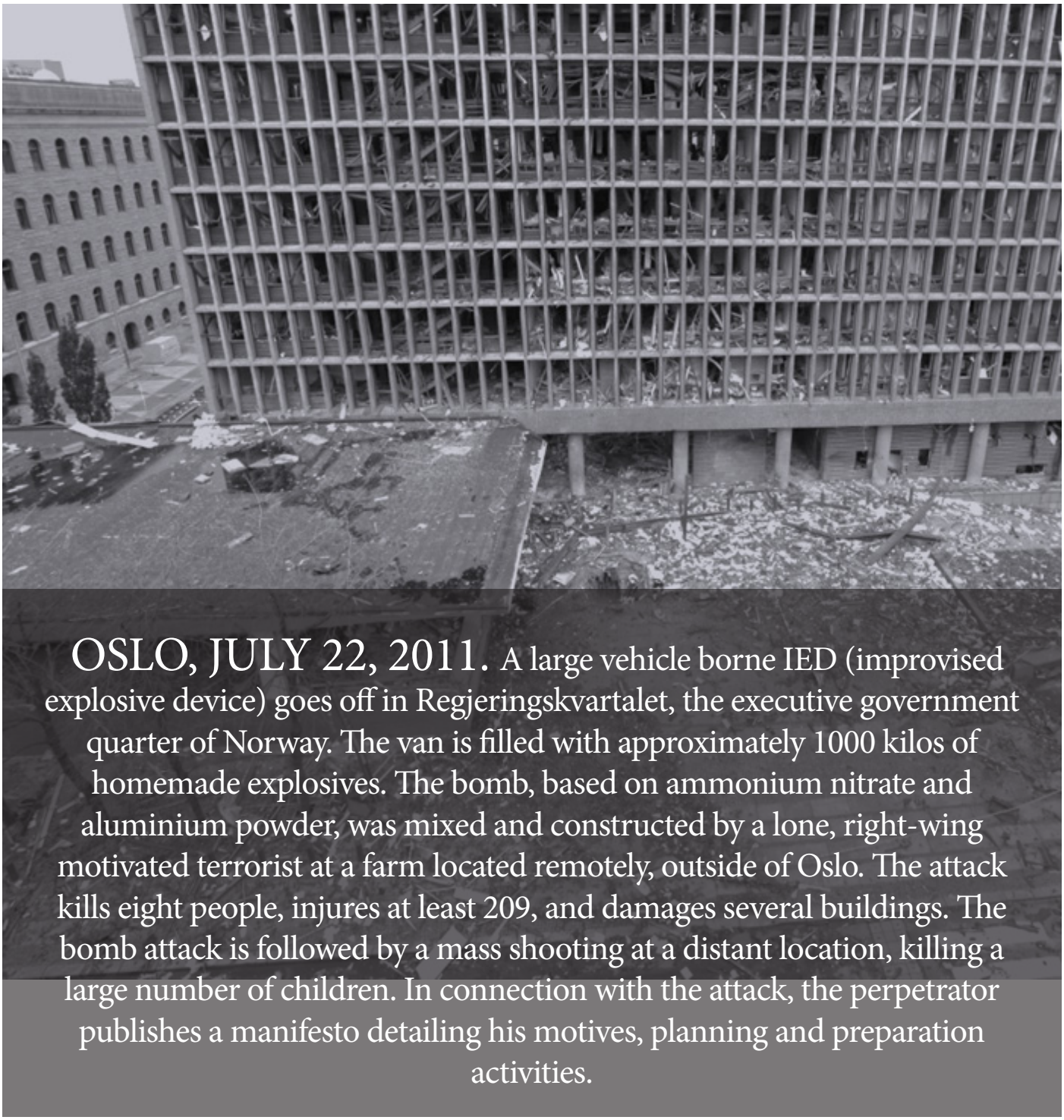
This report summarises the outcomes of EXERTER from our work with a scenario based on the Oslo bombing in 2011. It presents the findings related to the different counter attack domains and presents the concluding analyses and recommendations on future possibilities and needs.

In the beginning of EXERTER's yearly cycle, practitioners' requirements and gaps for countering the threat scenario was identified. These were based on analysis of input received from stakeholders and the expert community. The information has been collected in a classified report[1] and it has formed the foundation for the continued work.



[1] Please contact EXERTER for further details

The Scenario



OSLO, JULY 22, 2011. A large vehicle borne IED (improvised explosive device) goes off in Regjeringskvartalet, the executive government quarter of Norway. The van is filled with approximately 1000 kilos of homemade explosives. The bomb, based on ammonium nitrate and aluminium powder, was mixed and constructed by a lone, right-wing motivated terrorist at a farm located remotely, outside of Oslo. The attack kills eight people, injures at least 209, and damages several buildings. The bomb attack is followed by a mass shooting at a distant location, killing a large number of children. In connection with the attack, the perpetrator publishes a manifesto detailing his motives, planning and preparation activities.

Regjeringskvartalet in Oslo after the attack. Photograph: Kripos

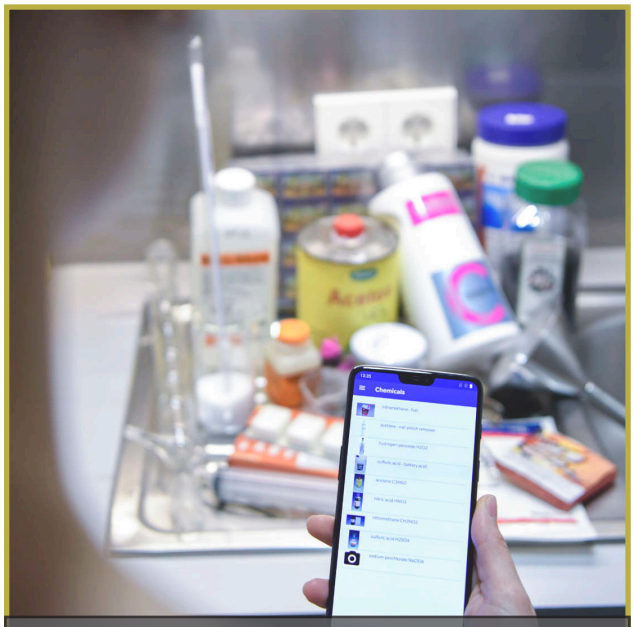
Prevent

The main part of the analysis for the Prevent domain is classified due to the sensitivity of the research in this phase of the time-line. Only a selection of the information is presented below. Measures for restricting the access to explosive precursors, and research on inhibition of precursors are some examples that are highlighted.

Research initiatives

For a scenario like the Oslo scenario, there are a number of past research initiatives relevant for the prevent domain. Some projects with focus on finding a bomb-making facility are for example BONAS, EMPHASIS and LOTUS, and research on inhibition of precursors, have e.g. been performed in EXPEDIA and PREVAIL.

There is also an ongoing project, XClanLab, with the aim to guide and support first responders in the identification of clandestine laboratories. The project further develops a mobile application, of which a prototype was developed in the project EXPEDIA. The tool contains different guides and can also put first responders in direct contact with experts. XClanLab held a presentation during the EXERTER Conference in Oslo.



XClanLab mobile application will guide and support first responders in the identification of clandestine labs

Photograph: BKA

Past research initiatives have for example:

- Studied techniques with potential to find a bomb-making facility
- Performed research on the inhibition of explosives precursors

Regulation and legislation

Explosive precursors are chemical substances that can be used for legitimate purposes, but they can also be misused for the illicit manufacture of homemade explosives (HME).

Legal actions to restrict the access to explosives precursors were, at the time of this analysis, described by Regulation (EU) No 98/2013 on the marketing and use of explosives precursors and by Regulation (EC) 552/2009, amending Regulation (EC) No 1907/2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH).

Regulation (EU) No 98/2013 restricts the access to, and use of, explosives precursors by members of the general public. It came into action after the Oslo bombings. If it had been in place in 2011, it could potentially have hindered the attack.

However, this provided that the purchases of e.g. sulphuric acid, which is included in the list of regulated substances, would have been reported, and investigated by the police in time to stop the attack.

During the work with the Oslo scenario in EXERTER there was an update of EU reg. 98/2013 in progress. Since the updates were not yet finalised the changes were not discussed or analysed.

The updated regulation, Regulation (EU) 2019/1148 on the marketing and use of explosives precursors, introduces further restrictions for the members of the general public to obtaining access to chemical substances that can be used for the production of home-made explosives. The regulation entered into effect on 31 July 2019 and shall apply from 1 February 2021. To monitor outputs, results and impact of the regulation, a monitoring program is established, and an evaluation will be carried out by 2026. Implementation of and enforcement across member states are central aspects for regulations to have the desired effect.

EU reg. 98/2013 contains two different categories of substances:

- Restricted - those that shall not be made available, possessed or used by members of the general public, and
- Regulated - those for which suspicious transactions should be reported

Detect

In the Oslo scenario the detect domain considers detection of Vehicle borne improvised explosive devices (VBIEDs) and ammonium nitrate based homemade explosives (HMEs) in a short time-frame. There are several different possibilities and approaches to identify a suspicious vehicle, and a selection of them is presented below.

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

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

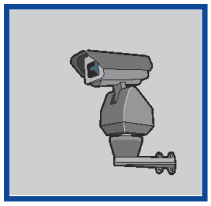
A number of different tools could be applied for vehicle screening at a checkpoint location. Some of these already exist and simply require promotion and dissemination, others do not exist or require further development.

In general, there is a lack of suitable detection equipment, and thus a need for research into new detection technologies and novel ways of using existing technologies and combinations of technologies.

A suspicious vehicle could be identified by:

- Driver identification with recognition
- Trace detection of solids or vapours
- Bulk explosives detection
- Device component detection
- License plate security cameras

Research initiatives



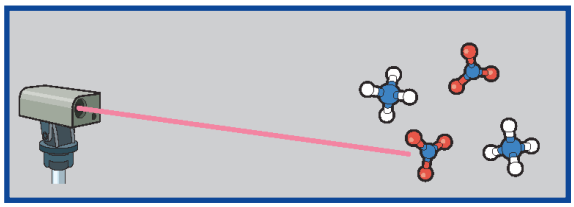
At European level, there are several research initiatives where the developed tools could potentially be applied for vehicle screening. Some European projects that are partially applicable to the Oslo scenario are the projects C-BOARD, EFFISEC and IMSK.

C-BORD worked with generalised inspection of container and large-volume freight. The applied techniques were radiation detection, Cargo X-Ray, Tagged Neutron Inspection, Photo-fission and Biosensor arrays for vapour detection.

EFFISEC focused on integrated security checkpoints. The project aimed at developing technology for automatic gates, portable identity check and scanning equipment to be used for in depth controls of travellers, luggage and vehicles, for pedestrians and people inside vehicles.

The last project, IMSK, focused on mobile solutions, and covered technologies for e.g. area surveillance and security checkpoints. The system was to allow rapid deployment at venues and sites (hotels, sport/festival arenas, etc.) which temporarily

need enhanced security. The employed technologies were various new sensors for threat detection and validation, including cameras (visual & infrared), radar, acoustic and vibration, x-ray and gamma radiation.



Requirements on technology

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

Screening processes could include standoff detection of trace contamination, vapour detection technologies and techniques for detecting concealed explosives whilst the driver and passengers are in the vehicle.

Some requirements for vehicle screening technology are for example that it should be easy to use with minimal operator training, and that it should be applicable to any of the types and sizes of vehicles likely to be encountered. The technology should also either be able to screen as much of the vehicle as possible or specific areas can be pre-determined for screening (such as door handles and other primary contact points).

Development possibilities

A selection of various tools and methods that could be developed to potentially generate an improved situation for the detection of VBIEDs are listed below.

Training:

- CCTV operatives and security staff to identify suspicious behaviour related to IED attacks
- First responders identify and notice the presence of potential secondary devices
- Training courses and guidelines for vehicle screening operations

Automatic license plate and vehicle security cameras:

- Database system for automatic identification of vehicles (ability to alert for various events)
- Automatic alert in case of presence of an unauthorized vehicle
- Information (e.g. illegal parking) shared with LEA officers

Methods to identify suspicious behaviours (people, vehicles):

- New ways of raising citizens' awareness
- Develop automatic systems for controlling and reporting.

Driver Identification and facial recognition with CCTV system:

- Database of names (suspicious people, vehicles)
- Quick information shared with LEA officers

And finally, stand-off detectors (traces, bulk, anomalies, non-chemical components, etc.) (e.g. for unusual chemical signals)

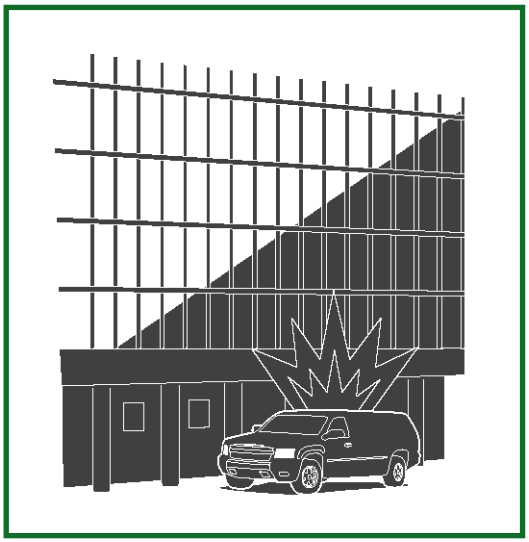
Mitigate

Below, mitigation of the effects from a VBIED in an urban environment is addressed. Some different technical solutions for physical mitigation measures are noted to exist and a selection of research initiatives on the topic is presented. Outlined are a few examples of future possible opportunities and initiatives in the mitigation domain.

Several research initiatives have addressed possible mitigation measures to 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.

Research initiatives

Past research initiatives that address aspects of improving mitigation of explosion effects are 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 examples of 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.



Needs and possibilities for mitigating explosion effects

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 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 maintaining 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 are e.g. developing mobile structural components to reduce blast effects, improving the 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.

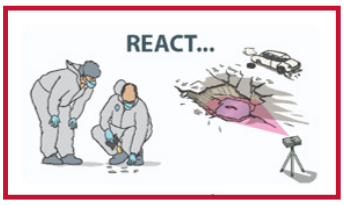
In terms of exploiting research results, there is a need to put more emphasis on transferring the knowledge gained within the research projects to potential end users. This includes making results more accessible technically, but also on a "language level" that enables end users to directly transfer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

At the EXERTER Conference in Oslo, 2019, the rebuilding of the governmental headquarters in Oslo was discussed as one example of when a balanced approach between security, functionality and cost is used. For achieving a targeted security level, risk assessments and threat level assessments are used as a part of the building design process.

Examples of possible future initiatives:

- Developing procedural standards, design guidelines and certification of protection guidelines
- Developing mobile structural components for reducing blast wave effects
- Process to integrate physical security into the common design process
- Making existing solutions available and research results easily accessible to end users
- Basic research on physical security aspects of new façade components and load bearing

React



The react domain covers emergency management, spanning everything from interaction between different organisations at the site and risk minimisation for first responders, to crime scene investigation. An overview of research initiatives in this domain and a selection on future development possibilities are given below.

Research initiatives

There are a number of past research initiatives in this domain for the Oslo scenario. For example, ACRIMAS and BRIDGE addressed crisis and emergency management, and E-SPONDER worked with information and communication support to first responders that act during abnormal events occurring in critical infrastructure.

Others are SAVASA, that worked with creating a video archive search platform, and FORLAB, HYPERION, ROSFEN and SUSQRA that addressed different aspects of evidence collection and evaluation.

Needs and Possibilities

Due to large differences regarding national and local frameworks, procedures and the structure of law enforcement agencies and emergency services, and 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 among different countries, applicable standardisation which comes into place in the aftermath of an extensive emergency is scarce. Nevertheless, several research projects deal with the topic of crisis management. It is unclear to what extent these research efforts can be or are being transferred into standard operating procedures and put into practice.

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

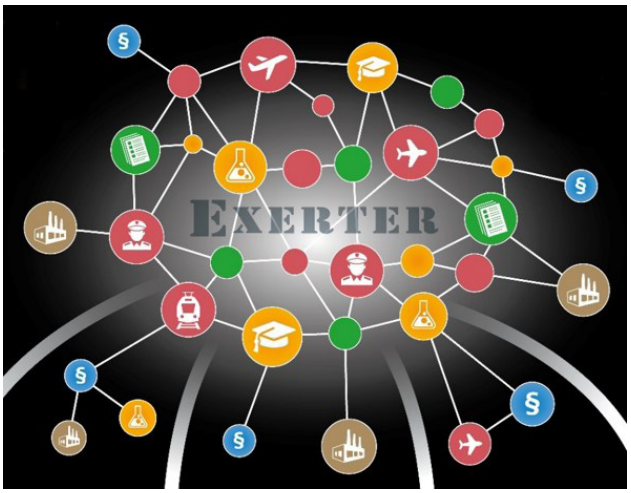
Forensic work after the Oslo attack
Photograph: Oslo policedistrict

Concluding remarks

The counter attack domains address different aspects of the scenario, setting a wide perspective on countering an attack by explosives. This summary aims to give some insight in, and an overview of, the field, and the material in it is based on discussions within the project and brief analysis of the respective domains.

The summary is not claiming to be all-covering and in-depth, both due to security classification reasons, and due to that EXERTER's focus is information sharing and networking rather than detailed analysis.

For each domain, this summary presented a selection of past and present research initiatives that are relevant for this scenario, and some needs and requirements as well as future possibilities to counter it. The Prevent domain centred around EU-regulations, and in Detect research on explosives detection as well as automatic identification of vehicles and suspicious behaviour was mentioned as some future possibilities. For the Mitigate and React domains, making technology and information available to end-users and the implementation of existing knowledge in standards, guidelines, and processes were some of the notes that were made.



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

Consortium

www.exerter-h2020.eu