Scenario: Criminal use of explosives

The fourth 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: Criminal use of explosives -
The fourth annual report in EXERTER

FOI-2017-1045
June, 2022

Photo: FOI

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, thus enhancing the overall Security of Explosives. The core of the EXERTER network brings together experts from Law Enforcement Agencies (LEAs), 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 threats, the related operational requirements on methodologies, tools and technology, and the status in research and innovation, EXERTER provides practitioners with the operative knowledge and tools for enhancing the security of our society.

Each year, EXERTER focuses on a scenario or set of scenarios with connection to Security of Explosives. The scenario is a plot defined from planning to execution of an attack, and is used to identify weaknesses in our response as well as potential countermeasure improvement. Focus is on the areas standardisation and certification, research and innovation, and exploitation.

The scenario for year four in EXERTER revolves around the criminal use of explosives. A summary of the work, analysis, and recommendations related to this year's scenario is presented in this report.

Information in this report is collected from EXERTER report D6.8 - 8th Report on Innovations, Standardisation and Exploitation within SoE, v1.0, June 2022

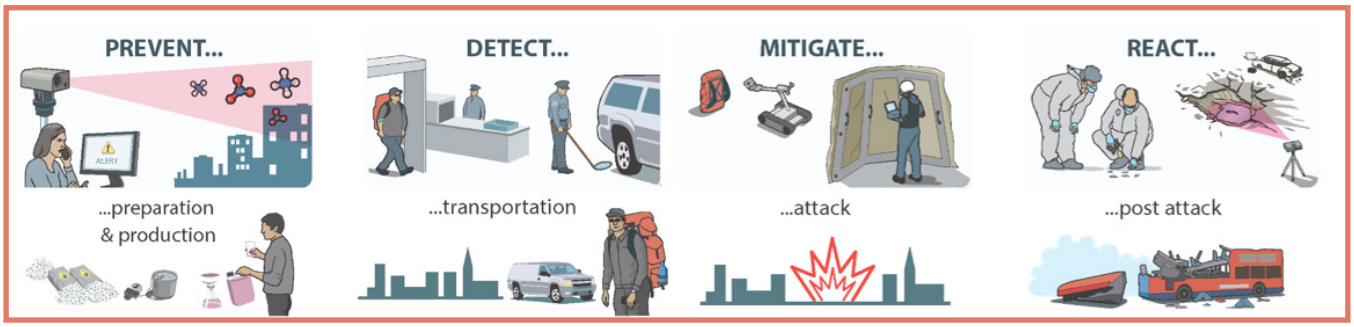
Introduction

Each year, EXERTER defines a scenario or set of scenarios, 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 the work with scenarios involving the criminal use of explosives. 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 were identified. These were based on analysis of input received from stakeholders and the expert community. The information has been collected in a classified report and it has formed the foundation for the continued work.



Scenarios

The scenarios revolve around the illegal use of explosives. The motives vary. Unlike terrorists, the ultimate aim is to maximise profits and reduce risks, rather than to draw attention to themselves.

Financial gain

Robbers attack an ATM for cash. The denotation leads to partial destruction of the ATM safe, and fragments reaching 200 meters, hitting a passer-by.

A gang extorts local businesses for 'protection money'. They extensively damage one shop owner's car by initiating a small pipe bomb and a banger.

Power gain

A gang member initiates an improvised explosive device (IED) via a black powder fuse at a residence building entrance to eliminate an enemy.

A gang revenges a theft by placing a timed blast incendiary at night on the windowsill of a bedroom window.

To intimidate a witness a low-level home-made explosive (HME) is detonated outside the witness' house.

Personal gain

Misuse of pyrotechnics for fun – A football supporter smuggles flash-bangers into a football stadium and lights them. Some bangers cause injuries to bystanders; burns to the skin, damage of hearing and cuts due to fragments from the bangers.

Prevent

This chapter offers suggestions to reduce the risk from the criminal use of explosives; it tries to address the issue before anything illegal happens. Since this is an international topic, an approach could benefit from being taken at a European level. Furthermore, we describe how legal users of explosives, for instance, the mining industry, could play an essential role in crime prevention.

Regulation & Legislation

Past cases where explosives, precursors, and pyrotechnics have been used to cause harm, by accident or on purpose, can illustrate the risk level to legislators, manufacturers and the public. Laws and regulations governing explosives, precursors, and pyrotechnics have been extended and become stricter during recent years. However, there are still actions that can be made to further prevent criminals from using them.

For instance, EU could harmonise procedures for cargo checkpoints to prevent commercial and military explosives from being imported or smuggled from other countries. A unified European approach in legislation that specifies the type of legal products and limits their size could potentially reduce smuggling of pyrotechnics. A harmonised legislation could also include e.g. grading sentences for possession of pyrotechnics according to the damage potential.

Photo: MONUSCO Photos, CC BY-SA 2.0, https://creativecommons.org/licenses/by-sa/2.0, via Wikimedia Commons

Photo: FOI

Surveillance of open sources (e.g. social media) could be considered to reduce the access to instructions on the internet on how to make explosive charges. The legal framework for securely storing and handling mass data must then be considered, along with privacy issues.

Furthermore, regulations on businesses that legally use explosives (e.g. construction- and mining industry)

Possible suggestions to improve prevention:

- Harmonised European pyrotechnic legislation to sentence according to damage potential and checkpoint procedures to reduce smuggling
- Stricter explosives control in the industry to minimise theft and illegal trade, regular background checks of employees, and improved reporting of missing explosives
- Improved communication within institutions, between LEAs, between the military and civilian sectors, and on an international level
- Increased internet surveillance to spot preparation instructions for explosive charges

could be increased regarding access requirements in order to reduce theft and illegal trade with explosives. Making regular background checks of all employees with access to explosives mandatory, and following procedures for immediately reporting and investigating missing explosives are other efforts to reduce illegal use of explosives.

Research Initiatives & collaboration

There is typically an excellent response rate and communication during and after crisis events, but sometimes a lack of communication in the prevention phase. Hence, communication could improve within institutions, between LEAs, between the military and civilian sectors, and on an international level to hinder/stop attack plots at an early stage.

The identified research initiatives mainly fall into three focus areas: collaboration, video surveillance, and analysis.

Several research projects revolve around improved collaboration between different LEAs and between the police and the public. CAPER, helps prevent organised crime through a platform for sharing, exploitation and analysis; INSPEC2T improves collaboration between police and the community; and UNITY involves the community in identifying policing priorities.

SAFEPOST raised postal security by screening parcels and TAKEDOWN analyses the dimensions of organised crime and terrorist networks

Video surveillance is the common focus of SMARTPREVENT, VALCRI and VICTORIA. SMARTPREVENT exploits the full potential of video surveillance, VALCRI analyses footage for sense-making in criminal intelligence analysis, and VICTORIA analyses videos for criminal and terrorist activities.

Detect

The discovery of a planned, ongoing, or concluded act of crime is one key element in the chain of crime-fighting. To detect the criminal use of explosives, here, we illustrate possible technologies that range from surveillance technology that automatically assists trained human operators to sensors that allow the detection of explosives from a distance.

Research Initiatives

Identified research activities for the detection domain cover e.g. surveillance technologies and algorithms for data analysis.

The EU-funded project CoESS works on training of Explosive Detection Dog (EDD), other projects such as CHEQUERS, MiRTLE, STANDEX and DEXTER have worked on identifying explosives and weapons in different environments. There are also several research initiatives around CCTV and other surveillance systems, such as the EU-funded AWARE project.

Challenges & Possibilities in Detection

The scenarios present a wide variability in the modus operandi on how an attack could be potentially performed, making identifying detect solutions challenging. The detection phase for some of the proposed scenarios might be the weakest link in the C-IED chain for some of the proposed scenarios.

Moreover, detection technology might not be the optimal solution for some scenarios because it would require training, well-developed and exercised SOPs, and mechanical and logistic support. For some of the selected scenarios cost-effective measures that can be widely and easily implemented,

Identified reaserch suggestions:

- Innovative crowd behaviour analyses
- Tool to accelerate video analysis
- Video surveillance technologies to assist operators of critical infrastructure
- Operators' needs for explosives detection at locations that have a secure perimeter
- Guidelines for preventing ATM attacks and for physical ATM security
- Training of the staff who perform real-time monitoring of building alarms and CCTV covering the area around an ATM
- Raising quality in Explosive Detection Dog (EDD) services
- Key principles and guidelines on the use of EDD
- Automated dog trainer devices
- Contactless close- and long-range sensors for trace explosive detection on surfaces and concealed threat detection.

and give a real benefit, could for example be increased awareness of indicators of IED emplacement, and improved surveillance with CCTV and EDD. Indicators of IED placement may

Photo: FOI

be detected by routine law enforcement activities that can intervene to prevent imminent bomb threats and stop the placement of a device. Security personnel or citizens may also be able to observe suspicious activity, such as someone leaving an unattended bag at a site, and notify authorities.

Exploration & Development of New Technology

A critical aspect to consider during the development of new technology for the detection phase is the ability to quickly adapt to the continuous development of the modus operandi regarding the methodology to perform an attack.

It is also important to consider and address the factors that might hinder the adoption of innovation (e.g., fragmentation of the market, low market visibility, cultural barriers on the demand side, and ethical and legal societal issues). It should be noted that innovation uptake can be a slow process full of decisions, usually taken by the buyers.

Together with the technical development of new technology, its validation for the intended use and the cost-effectiveness assessment, some ideas which have been brought up for actions could be EU standardisation activities to best support user need, and enabling of common access to data sets at the EU level.

Collaboration

Not only government initiatives (i.e., public funding or new legislation) are required for successful innovations in the long run. A successful future in the market can also depend on a genuine involvement, commitment, and partnership of potential clients in the security industry from the beginning. This would benefit a proactive collaboration between innovators and end-users of the technology.

Collaboration is essential to accelerate innovation at different stages and between various actors (e.g., governments, regulators, policymakers, industry, innovators, researcher teams, and users).

Photo: Harland Quarrington, OGL v1.0OGL v1.0, via Wikimedia Commons

Mitigate

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 available tool that can guide the decision process by balancing costs and effectiveness.

Research initiatives

Countering terroristic attacks in the mitigate phase at public spaces, critical infrastructures and buildings of interest is well-established and has been a major field of research in the past and now. For example, the RIBS-project supported the design of effective and viable integrated security measures protecting infrastructures without affecting their business dynamics. VITRUV (Vulnerability Identification Tools for Resilience Enhancements of Urban Environments) contributed to enabling the development of more robust and resilient spaces in the field of urban (re)planning/ (re)design/ (re)engineering. SPIRIT (Safety and Protection of built Infrastructure to Resist Integral Threats) aimed at developing tools to reduce damage, destruction, and disruption to large new and existing buildings.

However, the well-established measures and technologies that could be applied with respect to a large part of the scenarios are not really suitable since these attacks can occur everywhere, and a comprehensive implementation is not economically feasible. As such, these measures are also not mentioned in respective design- or building codes. Further research to handle these attacks in the mitigate domain does not appear as promising as research in other counter-attack domains.

Photo: redspotted from London, UK, CC BY 2.0, via Wikimedia Commons

ED Neutralization

Mitigating attacks by criminals through IED neutralization is from a technological point of view similar to terroristic motivated attacks. With respect to the neutralization of IEDs, SUBCOP developed technologies and procedures that can be applied by the Police Security Forces when responding to a suspected PBIED (Person Borne Improvised Explosive Device). In ENCOUNTER, besides innovative techniques for mitigation of IED effects, the neutralization of IEDs in urban/civil environment was investigated. The outcome of research projects and IED neutralizing technologies can help mitigate explosion effects in the criminal use of explosives domain.

Protection of ATMs

Technological and organizational solutions protecting ATMs and their surroundings from explosions effects are in principal available, but not widely applied due to financial reasons. ATMs that are targeted in attacks are typically just removed or moved to safer locations.

Evacuation

Regarding the scenario with misuse of pyrotechnics, preventive measures are strongly recommended and seem to be the most promising. To mitigate the physical effects of these pyrotechnics, using structural measures is probably not applicable or necessary because of the small effective radius of such devices (compared to larger IEDs with high explosives). These pyrotechnics can cause significant injuries to people in the close surroundings and e.g. cause dangers such as mass panics. Therefore, organizational measures such as evacuation could mitigate the effects of these attacks.

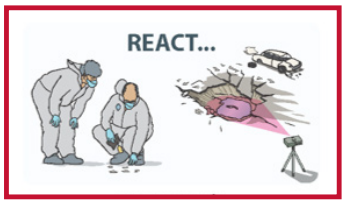
Further Research

A field for further research could be the identification of simple and cheap technological and organizational measures to mitigate explosion effects. The basis could be quantitative risk analysis, where different kinds of measures, their costs, and effectivity are evaluated against each other.

Possible suggestions to better mitigate the effect of explosives:

- Resilient and robust building solutions during urban planning and design
- Protect infrastructure (reduce damage and destruction) with business dynamics in mind
- Identify technological and organisational measures to mitigate explosion effects on ATMs
- Quantitative risk analysis to balance costs and effectivity
- Evacuation plans to mitigate secondary harm to a crowd in panic

React



The catalogue of potential options to react to the criminal use of explosives is broad; it covers legislation, police communication, surveillance of physical places and the cyberspace.

Challenges & possibilities in React

The different scenarios pose different challenges for the react domain. The scenarios with financial gain as motive, especially attacks on ATMs for cash, might be countered by improved CCTV inside and outside banks and ATMs. In addition to better surveillance, safety measures in the ATM could be enhanced by e.g. explosion- and flameproof enclosures.

To further discourage from ATM attacks, ATMs could be adapted to be able to invalidate banknotes by automatically staining them with paint and marking them with artificial DNA when they are subject to an attack. A priority is also the protection of ATM maintenance teams. The use of body- and dashboard cameras, mobile alarms or emergency buttons could have a deterrent effect, and might also provide information to the law enforcement, to intervene during the attack or as evidence afterwards.


Photo: Bernhard Zachhuber, FOI

One of the scenarios considers money extortion. Although the options to react to this scenario is seen to be limited, one possibility is for the police to establish or intensify communication and cooperation with local businesses (i.e., the victims).

In another scenario, explosives and pyrotechnics are misused for personal gain at a football stadium. To counter these incidents the entry controls and surveillance at stadiums could be intensified. Effective countermeasures from the detect phase which could also help in the react domain include specialised dogs, personalised tickets, and improved CCTV inside and outside a stadium. Improved communication between police, fans, and football clubs could also aid in countering this scenario.

For all scenarios that involve explosives stolen from an explosives storage, enhanced protection of these storages could provide an important

The following concepts are thought to allow to react better:

- Automated footage analysis that identifies relevant individuals and reconstructs a sequence of events
- Forensic lab that optimises evidence collection through in-situ evidence analysis
- 3D-scanner that records and analyses footwear and tyre impressions
- Development of analytical tools that chemically profile explosives in forensic casework

countermeasure. If combined with possibilities for tracking and tracing the explosives, the amount of used in IEDs might be reduced even further.

Improved and more extensive monitoring and surveillance of the trafficking of ammunition, pyrotechnics, and precursors on the darknet, could reduce the number of attacks. In addition, the surveillance of social media could be intensified.

Standardization and certification

Regarding classification and certification, higher requirements for dealing with and possessing specific types of pyrotechnics could limit the use. Currently, the classification of pyrotechnic products is not homogeneous throughout Europe, and one solution could include a unified European approach that classifies threats from commercial pyrotechnics via reproducible measurements.

Legislation and regulation

For increased legal certainty and more efficient processes, courts could have prosecutors and lawyers specialised in explosives and simplify access to expert advice from explosives specialists. Moreover, convicting evidence may be found faster through improved cooperation between organisations and authorities.

Photo: Public domain, via Wikimedia Commons. File:USMC-071129-M-1013R-004.jpg

Concluding remarks

During this last year, the EXERTER network has tried to find ways to interact and share experiences, despite the covid-19 situation preventing us from meeting. Two virtual workshops and a virtual conference provided a forum for many discussions and exchanges. National discussions were held with stakeholders and practitioners, resulting in many requirements and suggested recommendations for improvements.

The focus within the Prevent counter attack-domain this year was identifying research initiatives working on related issues, such as collaboration platforms for exchange of experiences, video surveillance, or detecting smuggling of explosives substances. Many of the recommendations lifted within the network this year concerned smuggling, legislation and education on the risks with, for example, pyrotechnics.

The Detect phase highlights research projects connected to improved canine detection, CCTV surveillance, and other detection methods for explosives and weapons. It lifts the importance and difficulty of detecting and identifying a threat and pinpoints some ideas for identifying or discouraging the perpetrator.

A challenge in Mitigation for this year's scenario is how to mitigate against a threat that can occur anywhere and in ordinary buildings. Many research projects and measures exist with the focus on mitigating effects on critical infrastructure and facilities of interest, but such measures would not be economically feasible to apply in general buildings. For the protection of, for example, ATMs, some ideas are lifted to mitigate the effects and concepts to limit the impact of pyrotechnics use.

In the React domain, a lot of focus was put on the importance of forensics analysis and improving communication between different actors. The aftermath of an incident is also closely connected to the other work on surveillance and on preventive measures to give a better toolbox to work with.

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

EXERTER consortium