

Welcome to the latest newsletter of EXERTER, an EU Funded H2020 project. EXERTER commenced in May 2018 and is a five year project which seeks to connect practitioners into a pan-European network of explosives specialists.

## Message from the Project Coordinator

EXERTER is now on it's final year, and will conclude with bringing in a wide and very interesting theme for this year's discussions. Finally we were able to meet at a physical project meeting in Madrid in May, where INTA hosted us and we all got to visit their impressive laboratories. Unfortunately the annual conference in April still had to be held virtually, but we hope that you all enjoyed the very interesting, informative and sharing nature of the presentations and interaction online.

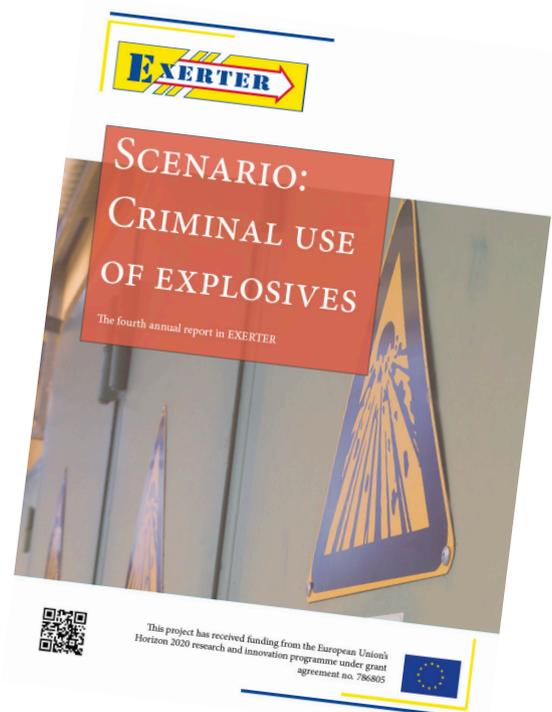
For this final year we sincerely hope that we will finally be able to both host our own workshop and conference physically, and also visit and participating in many events within the community. I think we all feel a fresh start now that we are finally able to discuss, learn and be inspired by all others in the networks through face-to-face meetings. All information on future plans and events will be sent out by email, and can be found on [exerter-h2020.eu](http://exerter-h2020.eu) and on the EXERTER linked-in page. I hope you will all keep interacting in our EXERTER network!

## EXERTER Annual Report

EXERTER have published the fourth Annual Report, titled 'Criminal Use of Explosives' in June 2022. You should have received a copy with this newsletter, however if not please email and a copy will be forwarded to you.

The report focuses on the research completed in year four relating to IED attacks for criminal purposes. As with previous years the report looks across the four attack phases, summarising the key findings. We hope you find it interesting and if you have any questions please do not hesitate to email the Project Coordinator.

Please feel free to share with you colleagues or wider network.



For more information visit:  
[www.exerter-h2020.eu](http://www.exerter-h2020.eu)

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



# EXERTER Virtual Conference 2022

Due to the ongoing pandemic, the EXERTER Annual Conference was again held as a virtual conference in April 2022.

115 participants attended to discuss and evaluate the year 4 core subject “Criminal use of Explosives” from multiple perspectives in connection with the counter attack domains of Prevent, Detect, Mitigate and React.

The conference started with a presentation of the results of the EXERTER National Workshops on the year 4 topic. The purpose of the workshops was to contribute to the progress by discussing requirements, need and issues connected to the scenario, to make sure, development was based on reality. The general aim was to give input to important questions related to the EXERTER counter attack domains Prevent, Detect, Mitigate and React, to be lifted within EXERTER and in a wider European perspective.

A hazard assessment regarding the misuse of pyrotechnics focused on the categorisation of pyrotechnics and the “cold pyrotechnic”. By the evaluation of the explosive contents, combustion temperature and reaction products it became clear that this kind of pyrotechnic is still a very dangerous article if misused in confined areas.

The importance of explosive detecting dogs in the context of criminal use of explosive was shown by the presentation of the recent research and development on training aids for explosive detection dogs. Tests with phlegmatizer were as well presented as the effectiveness of 2D-printed explosives reward samples for passenger screening dogs. Also the issue of rapid changes in scent profiles from stored explosives was discussed.

Case studies regarding attacks on ATMs and gang crime committed by criminal use of explosives, gave an impression of the police’s daily struggle with this topic.

A manufacturer presented their ATM crime deterrence technologies and explained, how the rapidly increasing number of and the dangers emanating from attacks on ATMs was countered by their technology.

How home-made explosives in a not initiated Improvised Explosive Device can be linked to a suspect by means of chemical profiling was also topic at the conference.

The conference concluded with an outlook for the EXERTER year 5 scenario “Influences emanating from conflict zones and operational theatres” by outlining numerous potential attack scenarios, based on the development forced by need, the distribution of explosives and emerging threats in the context of the EXERTER domains of Prevent, Detect, Mitigate and React.



© Europol

Keep an eye out in future newsletters for details on the EXERTER Conference 2023, which will consider the findings from Year 5 of the project.

More details on future EXERTER events, as well as reports and information can be found by visiting the project website at [www.exerter-h2020.eu](http://www.exerter-h2020.eu).

# ATM Explosions - A Plague across Europe

Rui Pereira - Feerica

Although crime around ATMs has been around for a long time, the latest data released by E.A.S.T. reveal a dramatic scenario, estimating more than a thousand ATMs exploded in Europe alone during the year of 2021, with Germany being the current epicenter of the problem with 400 explosion incidents reported that year.

But how did ATMs that have long provided convenient access to cash and other banking services become potential ticking bombs in our city centers?

And how did Europe become the epicenter of this plague, with hundreds of explosions taking place in highly populated areas, with several fatalities among innocent citizens?

To answer these questions, it will be important to understand how the different ATM protection strategies are related to the evolution of the various criminal Modus Operandi used over time. In fact, ATMs have always been highly attractive targets for criminals given the known existence of significant amounts of cash inside them.



The security industry was concerned with developing adequate countermeasures for this purpose. As a rule, the types of attacks based on hack tools, usually carried out in off-premises ATMs in remote areas, were avoided with the installation of alarm systems with remote monitoring, CCTV's or even hardened safes.

On the other hand, Ram-Raids were generally fought with the adoption of effective systems for anchoring ATMs to the ground, bollards to prevent vehicle access or, more recently, with GPS trackers that allow the tracking and recovery of equipment by law enforcement in a short space of time.

Although all these security systems have demonstrated their effectiveness in creating barriers and added difficulties to criminal activity, with numerous case studies proving the effective reduction in the number of attacks and success ratios, there were a small number of markets that opted for a distinct strategy – the destruction of money through IBNS systems (Intelligent Banknote Neutralization System) in case of attempted theft or violation of the equipment.

This was the case of the Portuguese bank Millennium BCP, which, in response to the exponential increase in the number of attacks on its ATMs following the introduction of the EURO, adopted this technology in 2006 to protect ATMs identified as being of high risk, having practically eliminated the incidence of theft on their network. Given the success of this initiative, most of the remaining Portuguese banks would follow the same strategy, having reduced the incidence of thefts in ATMs protected with IBNS to residual levels.

However, ATMs proved too attractive for criminals to give up on them, and a new technique for attacking ATMs was developed: Gas Explosions. This new Modus Operandi proved to be extremely effective, being able to successfully overcome all the security systems used until then to protect ATMs, making each once again a potential target for robbery, regardless of its location, protection systems, brand, or model.



The ODYSSEUS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021857. Project materials reflect only the authors' view and European Commission is not responsible for any use that may be made of the information it

To make matters worse, the gas explosions proved to be highly destructive and dangerous, marking the beginning of a new reality: The willingness of criminals to risk their own life to get the reward waiting for them inside the ATMs.

From this moment on, crime gangs could only be stopped by arrest or potentially getting killed in the process, marking a new and unprecedented escalation of violence around ATM attacks. The high media coverage of this type of incident also caused another highly unwanted side effect: the multiplication of individuals and criminal groups trying to reproduce and improve the execution of this type of Modus Operandi.

This perfect storm scenario created a great need for new security solutions that could protect ATMs against this type of incident, and the industry responded accordingly, developing different approaches and solutions for this type of problem.

In general, the response to gas explosive attacks created two distinct strategic lines, the first focused on preventing or mitigating the effects of the explosion, using explosion-proof gas safes and explosive atmosphere detection and inhibition systems, while the second focused on eliminating the reward through a new generation of IBNS, certified by independent entities through rigorous testing and evaluation methods, in order to guarantee its ability to withstand explosive attacks and guarantee the total destruction of cash in the ATM.

As examples, in explosion prevention adoption we can mention the Netherlands, while IBNS protection was regulated and made mandatory in France, with both models demonstrating their effectiveness against this type of attacks.

But once again the criminals developed and perfected a new attack technique, the “Pizza Slice”, this time using solid explosive shaped to facilitate the introduction inside the ATM safe after the violation of the banknote exit shutter.



The IBNS systems proved to be able to respond effectively to this new Modus Operandi, so the number of attempted attacks using this technique in markets where this type of technique was adopted was residual and unsuccessful.

To date, no other solution has proved to be effective against this and earlier attack techniques, except for IBNS systems, which once again prove their versatility, responding adequately to the evolution of attack Modus Operandi.

The IBNS technology has, therefore, a double effect, curative, and preventive, since it has proven effectiveness in reducing attacks in a first stage, and later acting as a crime vaccine, effectively immunizing against new Modus Operandi that may be developed by criminals.

France and Portugal are two well-known case studies that clearly prove the capabilities of IBNS systems, with a growing recognition of the capabilities of this technology among police forces, of which we highlight Europol, which in its White Paper dedicated to the protection of ATMs against physical attacks, clearly confirm the effectiveness of this type of systems:

*“Intelligent banknote neutralization systems (IBNS) are a first technique for spoiling the rewards”*

*“Best practice shows that IBNS can be very effective”*

Over recent years, the Dutch authorities have been able to reverse the growth of ATM attacks through a wide range of preventive measures, with a clear paradigm shift from the previous ATM protection strategy in favor of IBNS technologies, with a clear decrease in the number of incidents and an increase in ATM number protected with IBNS.

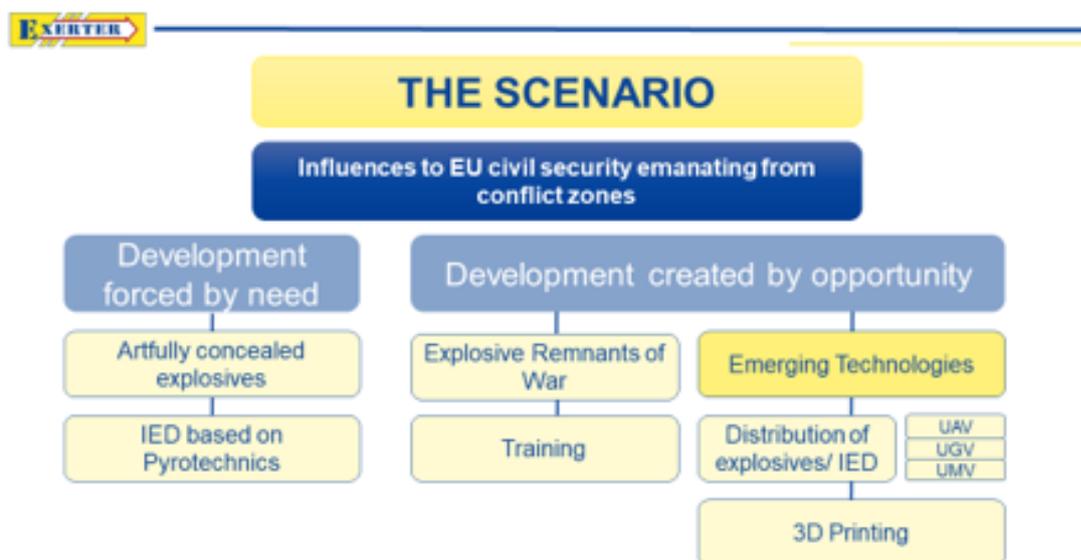
The effectiveness of these systems has also not gone unnoticed by the Croatian and Polish authorities, who have recently adopted security regulations for ATMs, in which the implementation of IBNS systems plays a central role.

It is important that countries that currently suffer from high rates of ATM attacks are aware that although attacks on ATMs is a complex issue, a solution to reduce and prevent this type of incident already exists, having been successfully proven in numerous markets – the IBNS systems.

Experience shows that any weaknesses in the ATM protection model will sooner or later be exploited by criminals, therefore we need to ensure we are always two steps ahead criminals, never a step behind. Current IBNS technology ensures that criminals have no reward, whatever they try, use or do, and are capable of providing law enforcement agencies with the required intelligence support, like real time attack awareness, online GPS tracking of stolen assets to get criminals arrested and irrefutable forensic evidence for effective court of law convictions, taking them out of action before they get killed or kill someone innocent in the process.

You can get more information on IBNS or Feerica at <https://feerica.com/>

## EXERTER workshop 2022 - Belfast



This year the EXERTER partners are delighted to announce that they are planning to hold a physical Workshop for the first time since 2019. The EXERTER workshop 2022 will take place in Belfast, Northern Ireland, and is planned for 25th - 26th October 2022.

This year's workshop will cover a broad field of topics included in the scenario as indicated in the diagram above. It will focus on influences to EU civil security emanating from conflict zones. The preliminary program consists of presentations and discussions on the subtopics;

- Explosive Remnants of War;
- Artfully concealed explosives/ 3D Printing (of explosives and charges),
- IED based on Pyrotechnics,
- Distribution of explosives/ IED (UAV, UGV, UMV) and ,
- Illicit training on the use and manufacture of explosives.

The workshop will be hosted by the PSNI and it is planned to include interesting visits to Police facilities and a Forensic laboratory. Registration will be open after the summer vacations and the final programme will be published, however if you have any queries, please do not hesitate to contact the organising team at [Euprogramme@psni.police.uk](mailto:Euprogramme@psni.police.uk).



The ODYSSEUS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021857. Project materials reflect only the authors' view and European Commission is not responsible for any use that may be made of the information it

# Networking & Events

## EXERTER Events

### EXERTER Workshop -

25th - 26th October 2022, Belfast.

For Registration information email - [euprogramme@psni.police.uk](mailto:euprogramme@psni.police.uk)

## Other Related Events

### ICBE 2022: 16. International Conference on Blasting and Explosives - 22nd - 23rd September 2022

London, UK

<https://waset.org/blasting-and-explosives-conference-in-september-2022-in-london>

### International Security Expo - 27th-28th September 2022

London, UK

<https://www.internationalsecurityexpo.com/welcome>

### BKA Conference - November 2022

Germany

### Home Office - Security and Policing Event - 14th-16th March 2023

Farnborough International Exhibition and Conference Centre, UK

<https://www.securityandpolicing.co.uk/>

### Fulmination 2023 - 18th -20th April 2023

East Midlands Conference Centre, UK

<https://iexpe.org/event/fulmination-2023/>

### Forensics Europe EXPO - 17th-18th May 2023

London, UK

<https://forensicseuropeexpo.com>

*If your project or organisation wish to promote a future conference, workshop or meeting please contact the EXERTER Project to have it included in future newsletters or the project website.*

## EXERTER End User and Expert Community

EXERTER End user and Expert Community (EEC) is important to the network, in order to give valuable input to scenarios, requirements, evaluations and upcoming threats.

It consists of practitioners, academia, research institutes, industry and policy makers. If you are interested in becoming a member of the EEC, or are aware of some- one who would benefit in participating in EXERTER, please contact the Project Coordinator. Alternatively if you only wish to receive regular information and updates on the project you can get this through visiting the website and the project news- letter. Please contact the Project Coordinator to be added to the project mailing list.

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



## Facts & Figures

Project duration:

01/06/2019 – 31/05/2023

Budget:

€ 3 498 868.75

## Contact

If you wish to find out more, are interested in our End user and Expert community or wish to receive the EXERTER Newsletter with updates of the project, please contact us:

[www.exerter-h2020.eu](http://www.exerter-h2020.eu)

Project Manager:

Anneli Ehlerding

Email:

[anneli.ehlerding@foi.se](mailto:anneli.ehlerding@foi.se)

Phone: +46-8-5550 3000



Security of Explosives pan-European Specialists Network

## Partners

