Title:	Document Version:
D3.7 Soft and hard mitigations	1.0

Project Number:	Project Acronym:	Project Title:
H2020-740466	LETSCROWD	Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs in mass gatherings

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type*-Security*:
M22 (February 2019)	M22 (February 2019)	R-PU

*Type: P: Prototype; R: Report; D: Demonstrator; O: Other.

**Security Class: PU: Public; PP: Restricted to other programme participants (including the Commission); RE: Restricted to a group defined by the consortium (including the Commission); CO: Confidential, only for members of the consortium (including the Commission).

Responsible:	Organisation:	Contributing WP:
A. Golfetti, S. Giorgi (DBL)	Deep Blue	WP3

Authors (organisation):

A. Golfetti, S. Giorgi (DBL); S. Allertseder (BayFHVR), C. Peres (ADM), J. A. Alonso Velasco (ERT), I. Jacobs (LPV), V. Da Silva Reis, P. Esteves Grilo (PSP); P. Townsend (CROWD); C. Dambra (PROPRS); C. Graf (RAILSEC); A. Cuesta (UC); A.G. Silva (ESYS); Giorgio Fumera (UNICA); A. Gizikis (EENA)

Abstract:

This document is the second version of the report on soft and hard mitigation measures. It presents an update of the mitigation measures reported in D3.3 including the new attack modes included in D3.6. In addition, the present deliverable reports the mitigation actions currently applied by LEAs to mitigate the negative effects of specific types of terroristic attacks.

Keywords:

Mass gatherings, soft and hard mitigations, risk assessment, security, prevention.

Revision History

Revision	Date	Description	Author (Organisation)
V0.1	03.12.2018	D3.7 Table of Content	A.Golfetti, S. Giorgi (DBL)
V0.2	05.12.2018	First contributions from LEAs and technology providers	S. Allertseder (BayFHVR), C. Peres (ADM), J. A. Alonso Velasco (ERT), I. Jacobs (LPV), V. Da Silva Reis, P. Esteves Grilo (PSP); P. Townsend (CROWD); C. Dambra (PROPRS); C. Graf (RAILSEC); A. Cuesta (UC); A.G. Silva (ESYS); Giorgio Fumera (UNICA);
V0.3	07.02.2019	First contributions from LEAs and technology providers	S. Allertseder (BayFHVR), J. A. Alonso Velasco (ERT), I. Jacobs (LPV); P. Townsend (CROWD); C. Graf (RAILSEC); A. Cuesta (UC); A. Gizikis (EENA)
V0.4	18.02.2019	Full consolidated draft	A.Golfetti, S. Giorgi (DBL)
V0.5	22.02.2019	Peer review	C. Graf (RAILSEC); Giorgio Fumera (UNICA); Agnes Hoechtl (BayFHVR)
1.0	27.02.2019	Final version	A.Golfetti, S. Giorgi (DBL)

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement № 740466.

More information available at https://letscrowd.eu

Copyright Statement

Executive Summary

This document represents the second version of the D3.3. - *Progress report on soft and hard mitigations* due (M12). Starting from the literature review carried out in D3.3, the present deliverable aims to report the mitigations currently used by LEAs to address the attack modes at first identified in D3.2 - *Progress report on dynamic risks for mass gatherings*, and updated in D3.6 - *Dynamic risks for mass gatherings*.

The deliverable is structured around three main sections as follows:

Section 2 – SUMMARY OF MITIGATIONS FROM D3.3

The first section synthetises the key findings came out from deliverable D3.3 - *Progress report on hard and soft mitigations.*

Section 3 - ANALYSIS OF LEAS CURRENT MITIGATION MEASURES

LEAs feedback was collected to combine the literature review carried out in D3.3 with the operational and expert perspective of the LEAs operators. To do that, six experts from different Law Enforcement Agencies within the LETSCROWD project were asked to fill in a structured template reporting the following information:

- Select the mitigation measures identified in D3.3 and currently used within their organisation (paragraph 3.1.1);
- List any other mitigations currently in place but not reported in D3.3 and add a short description of them (paragraph 3.1.2);
- Report any measures that would be useful to improve current operations and provide some ideas for new mitigations not in use (paragraph 3.2).

Section 4 - UPDATE OF THE LETSCROWD MITIGATION MEASURES

An update of possible mitigation actions linked to the LETSCROWD tools developed within the project was reported in this section.

While the majority of LETSCROWD outcomes could be potentially used to prevent specific terrorist attacks, the Dynamic Risk Assessment (DRA) and the Innovative communication procedures (ICP), as methodologies, are transversal to the different terroristic attacks and would apply to all of them.

Furthermore, even if not exhaustive, section 4.1 summarises a review of **long-term actions** undertaken at both European and National level to prevent the threat of terrorism such as:

- Building long-term partnership between private and public sectors in order to foster collaboration and cooperation, improve information sharing and knowledge exchange of global terrorism threat;
- Implementing and delivering of initial and continuing security awareness training courses for both practitioners and front-end operators working in crowded places and critical environments (e.g. transport hubs, hotels large arenas, cultural sites and shopping malls);
- Developing of a security culture involving communities and citizens.

Index

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 Purpose of the Document

This document is the second version of the deliverable on soft and hard mitigation measures. It presents an update of the mitigation measures reported in D3.3 (1) including the new attack modes included in D3.6 (2). In addition, the present deliverable reports the mitigation actions currently applied by LEAs to mitigate the negative effects of specific types of terroristic attacks.

1.2 Scope of the Document

The scope of this document is to identify soft and hard solutions usable to mitigate the vulnerabilities, threats and hazards identified and reported in D3.2 (3) and D3.6 (2). The main objectives of the document can be summarised as follows:

- Analysis of current LEAs mitigations measures;
- Collection of potential new mitigation measures;
- Update on the mitigation actions coming out from the LETSCROWD tools;
- Description of long-term mitigations to prevent the threat of terrorism.

1.3 Structure of the Document

The document is organized in 4 main sections:

- Section 2 synthesises the main key findings form D3.3;
- Section 3 presents an analysis of LEAs mitigation strategies based on the review carried out in D3.3;
- Section 4 includes an update of the potential mitigations coming from the LETSCROWD outcomes. It also comprises a short overview of some long term mitigation strategies – carried out at European level - to fight terrorism;
- Section 5 reports the main conclusions.

2 Summary of mitigations from D3.3

The deliverable D3.3 (1) - *Progress report on hard and soft mitigations* reports a list of possible mitigation actions to address specific attack modes identified in D3.2 (3). As mentioned in D3.3, it is typically not possible to eliminate all the risks associated with a given event. This implies that mitigation options must be carefully analysed, selected and prioritized. The selection should consider the following aspects:

- the mitigation measures that are more appropriate for the type of risks foreseen for the event under analysis;
- the resources and capabilities that are sufficient to implement the measures identified;
- the impact that the measures can have on the events and the area where it is organized.

Mitigations are not universal and shall be selected on the basis of the characteristics of the event because each event is different and the way it is organised, the location, the public and all its characteristics influence the effectiveness and appropriateness of the mitigations applied. The mitigations reported in D3.3 were discussed including the following aspects:

- a short description of the risk they address;
- a description of the worst-case scenario based on the literature review;
- a description of the possible existing mitigations actions available from the literature review, by detailing: the possible effect of frequency and severity, the potential adverse effect and the stakeholders responsible for the implementation of the mitigation.

The actions proposed were also classified in hard (HM) and soft mitigations (SM) according to what they concern and how they are realized, i.e.:

1. crime prevention through environmental design solutions– HM;
2. organizational actions – SM;
3. actions-based on personnel and related training - SM.

Table 1 reports the complete list of mitigations identified in D3.3, while a brief description for each of the mitigations is available in Annex 7.1.

Table 1: (Form D3.3.) List of risks related to terrorism and the proposed mitigations

Threat	Attack mode	Mitigations	Type of mitigation[1]
Terrorism	Vehicle used as weapon (vehicle ramming)	- Creation of vehicle exclusion zones by means of barriers	Hard (CPTED solution)
		- Sensitize and Training for detection of weak signals	Soft (action-based on personnel)
		- Control on vehicle rental and operation	Soft (organisational solution)
	Package Type IED	- Counter – IEDs awareness and training in suspicious behaviours	Soft (action-based on personnel)
		- Explosive detection systems	Soft (organisational solution)
	Vehicle-borne IEDs (VBIEDs)	- Counter – IEDs awareness and training in suspicious behaviours	Soft (action-based on personnel)
		- Vehicle surveillance and control/ inspection	Soft (organisational solution)
		- Anti-ram vehicle barriers	Hard (CPTED solution)
	(Squad of) Suicide bomb IED	- Counter – IEDs awareness and training in suspicious behaviours	Soft (action-based on personnel)
		- Physical barriers	Hard (CPTED solution)
		- Security and ID Checks	Soft (organisational solution)
		- Sniffer dogs	Soft (organisational solution)
	CBRN attack	- Chemical agents detectors	Soft (organisational solution)
		- Training for detection of possible attacks	Soft (action-based on personnel)
	- Cold steel and Cutting weapons	- Security Check at the event entrances	Soft (organisational solution)
		- Security Officers inside the Mass	Soft (organisational solution)
		- Setting major security measures along the event perimeters	Soft (organisational solution)
	Hijacking of social networks	- Improving the security of access to SNs	Soft (organisational solution)
		- Creating awareness on the use of trusted SN channels	Soft (action-based on personnel)
		- Identifying trusted channels for cultural minorities	Soft (organisational solution)
		- Counteract the spread of misinformation	Soft (action-based on personnel)
		- Mitigating the Crowd-turfing by the use of automated crawling systems that are able to identify fake messages	Soft (organisational solution)
	Shooting	- Body search	Soft (organisational solution)
		- Walkthrough metal detector (WTMD)/ X-ray scanning machine	Soft (organisational solution)
		- Training for identification of suspicious signs in behaviour and appearance	Soft (action-based on personnel)
	Combined attack	- Combination of several mitigations	

[1] In the deliverable D3.3 mitigation actions have been classified on the basis of the way they are realized. They can be based on:

- crime prevention through environmental design solutions (i.e. the environmental design to prevent crime) - Hard;
- organizational actions - Soft;
- actions based on personnel and related training - Soft.

See Deliverable D3.3 for a detailed description of each type.

(two or more attacks simultaneously launched against the event)

A preliminary list of mitigation actions coming from the LETSCROWD outcomes was provided in D3.3. D3.7 proposes an update of the mitigations supported by the LETSCROWD outcomes (e.g. tools/ software and methodologies) according to their current development status (see Section 4).

3 LEAs' current mitigation strategies: methodological approach

This section presents some strategies currently adopted by different Law Enforcement Agencies within the LETSCROWD project to mitigate the impact of specific threats. While the first version of the deliverable on soft and hard mitigation measures (see deliverable D3.3 (1)) was based on a top-down approach, focusing on a review of highly relevant sources and documentation (e.g. EU entities, security organisations, journals related to the security topic etc.) to identify the mitigation measures adopted to prevent the negative consequences of terrorist attacks.

Seven experts from five different Law Enforcement Agencies and one first responders participating in the LETSCROWD project (e.g. ADM, PSP, LPV, BayFHVR, ERT, EENA) were involved in the study. LEAs' operators were asked to fill in a spreadsheet template (see Annex 7.2) by reporting the following information:

1. Select the mitigation measures identified in D3.3 and currently used within your organisation;
2. List any other mitigations[2] currently in place but not reported in D3.3, and add a short description of them;
3. Report any measures that would be useful to implement and provide some ideas for new mitigations not in use.

LEAs feedback was collected to combine the literature review (top-down approach) with the operational and expert perspective of the LEAs operators (bottom-up approach). The information collected was used to:

- understand the mitigations currently applied by the LEAs to address a specific attack mode when organising a mass gathering event;
- validate and enrich the mitigation measures identified through the literature review;
- identify mitigation measures to support their current operations and ideas for improving what is still missing.

3.1 WHAT ARE THE MITIGATION STRATEGIES CURRENTLY APPLIED BY LEAs TO ADDRESS SPECIFIC ATTACK MODES?

The first part of the template aimed to collect the mitigation measures currently applied by the Law Enforcement agencies to address the attack modes identified in D3.2 and updated in D3.6.

3.1.1 Selection of the mitigation measures identified in D3.3 and currently used by the LEAs

Based on the initial review of mitigations (see Deliverable D3.3), LEAs were asked to select the most suitable mitigations (see Table 1) applied within their organisations and to include any other additional strategies currently used with a short description of them. A brief explanation of the answers has been reported for each attack mode.

Figure 1 reports the mitigation strategies adopted by LEAs to prevent and minimize the negative

[2] The mitigation measures collected through the study concern only strategies and recommendations that can be shared within the consortium without any problems. While information about police tactics and mitigation strategies are absolutely restricted and cannot be shared with anyone outside of the police.

consequences of a **vehicle ramming attack**. Results show that *barriers* positioned around vulnerable crowded areas and *training awareness for detection of weak signals* are adopted by the majority of the respondents to mitigate this type of terroristic threat. While the mitigation related to the *control on vehicle rental and operation* (e.g. mitigation actions concerning the procurement of the vehicle used for the ramming attack) is not a common procedure among Law Enforcement Agencies. One of the expert reports that a general control on car rental at national level is not applicable within his organisation due to national legislation constraints; however the police can require specific controls only in cases of suspects under surveillance.

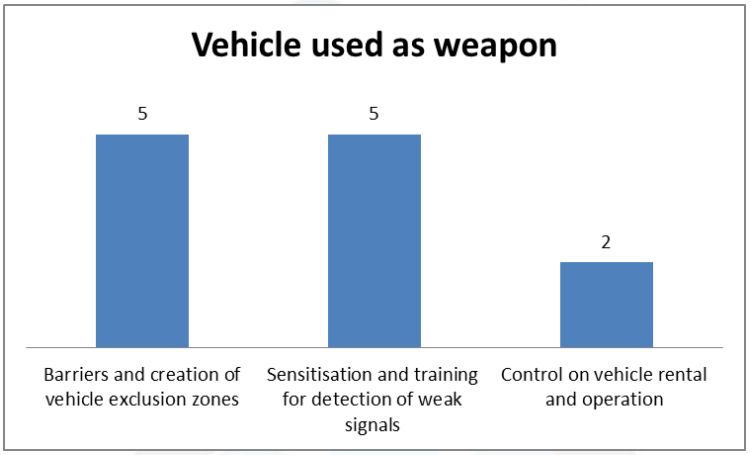

Figure 1: Vehicle used as a weapon - Level of adoption of the mitigations identified in D3.3

As mentioned in D3.3, **IED attacks** are difficult to prevent because they can be delivered in different forms, namely: package type IED, vehicle borne IED and suicide bomb IED. In general, *the training course for identifying and recognising suspicious behaviours* (Figure 2, Figure 3 and Figure 4) is a transversal mitigation action adopted by the majority of the LEAs representing the sample. Some experts highlighted that police officers only receive general operational courses that can include those topics. With this regards, the *LETSCROWD training package for crowd protection* (see D7.3 (4)- *Report on training package for crowd protection based on human factor* for further details) would represent a useful solution for the LEAs (see Table 5).

For preventing the risks of **Package type IED and vehicle borne IED** (Figure 2 and Figure 3), explosive detection systems, vehicle surveillance inspections and the anti-ram vehicle barriers seem to be widely adopted mitigations by all the experts involved in the study. While security checks and sniffers dogs are the most common solutions used to mitigate the effect of the **suicide bomb IED** (Figure 4).

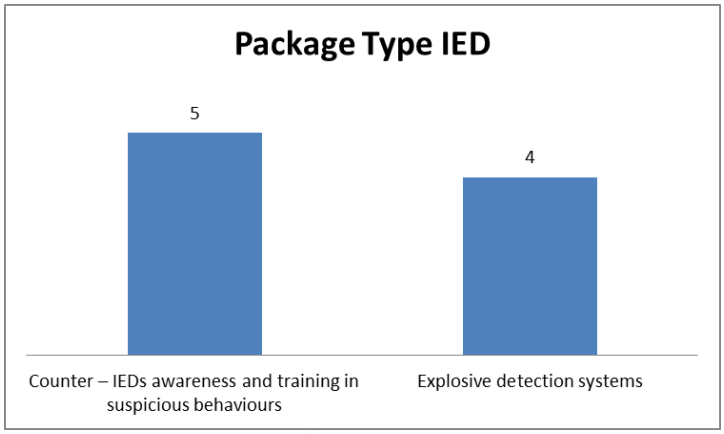

Figure 2: Package type IED – Level of adoption of the mitigations identified in D3.3

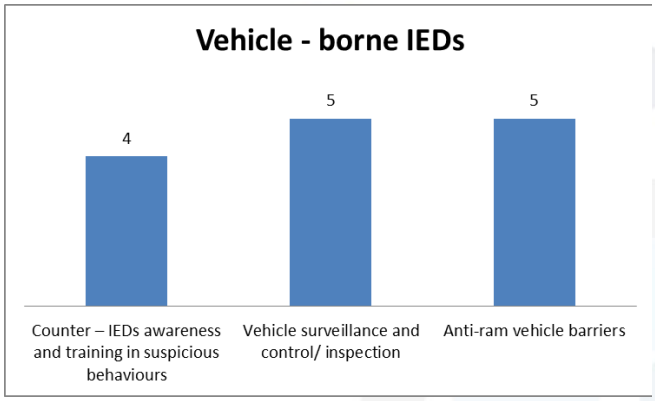

Figure 3: Vehicle – borne IEDs – Level of adoption of the mitigations identified in D3.3

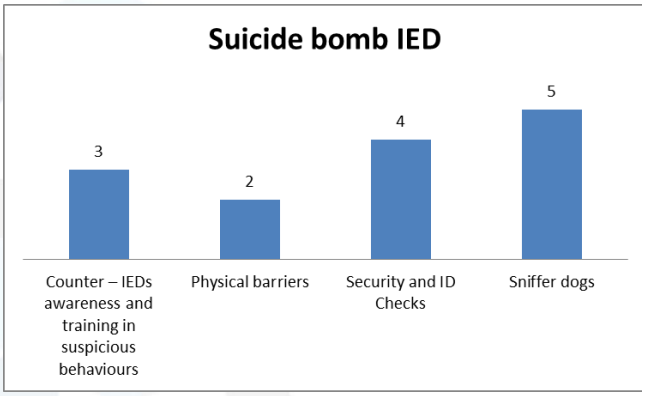

Figure 4: Suicide bomb – Level of adoption of the mitigations identified in D3.3

CBRN attacks are generally extremely difficult to prevent. Despite there is no evidence of chemical, biological, radiological or nuclear (CBRN) weaponry being used by terrorists in the EU, they represent a serious cause of concern to LEAs. As shown in Figure 5, LEAs adopt both *chemical agents' detectors* and *training courses to sensitise police officers to identify CBRN signals*. However, the majority of the experts underlined that the detection of chemical, biological, radiological, and nuclear agents often falls under the competence of the national Special Forces.

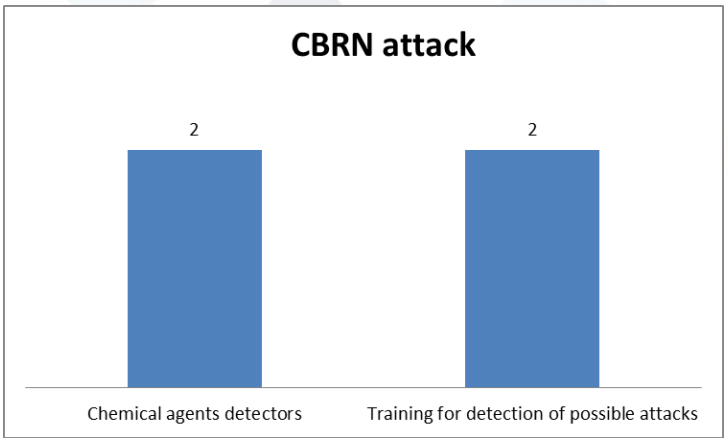

Figure 5: CBRN attack – level of adoption of the mitigations identified in D3.3

All the experts involved in the study agreed that the most effective ways to prevent cold steel attacks (Figure 6) concern the implementation of: 1) security checks at the event entrances; 2) security officers inside the mass and 3) security measures along the venue.

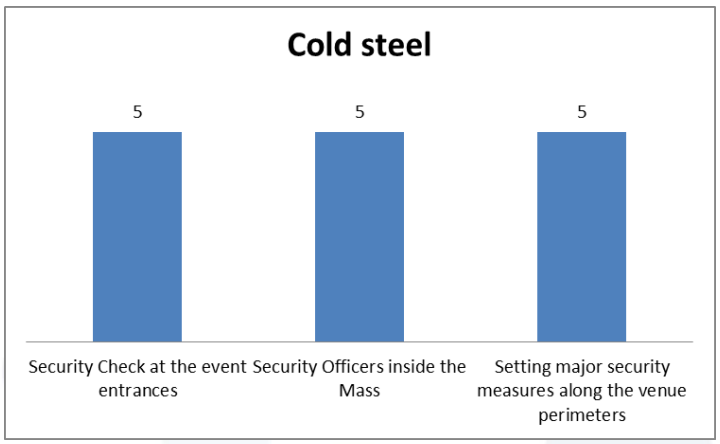

Figure 6: Cutting weapons – level of adoption of the mitigations identified in D3.3

For preventing the **hijacking of social network** the most effective action seems to be *the identification of trusted channels*, together with *awareness trainings* on the use of trusted social network channels to spread relevant information and *measures to counteract misinformation*. However, as reported in Table 3, these measures were also reported as mitigations to be improved by some of the LEAs.

Finally, as shown in Figure 8, *body search* and *walkthrough metal detector* are the widely adopted solutions to mitigate the **shooting attack**. As mentioned for the IEDs attacks, some experts highlighted that usually police forces do not receive a specific training on the identification of suspicious signs and behaviours.

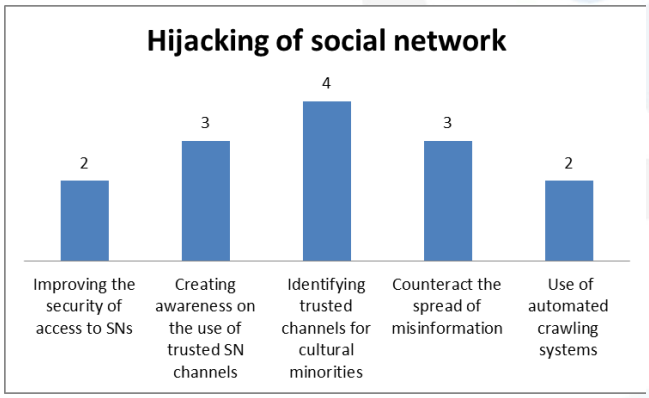

Figure 7: Hijacking of social network – level of adoption of the mitigations identified in D3.3

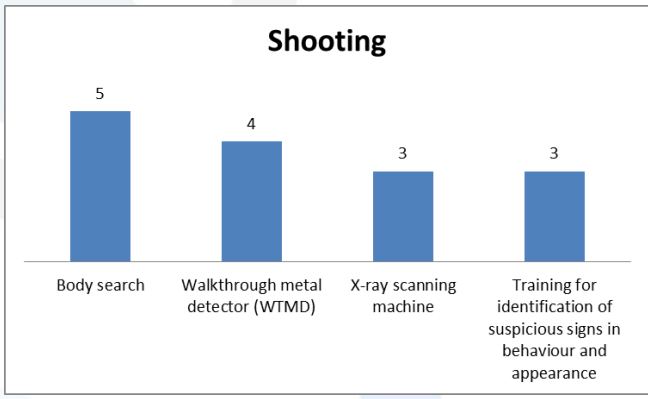

Figure 8: Shooting – level of adoption of the mitigations identified in D3.3

3.1.2 MITIGATIONS NOT IDENTIFIED IN D3.3 BUT CURRENTLY IN PLACE

LEAs were also asked to indicate any other additional mitigation actions currently adopted within their organisation to prevent the risk of the attack modes identified. The following table summarises the main input collected.

Table 2: Additional mitigations suggested by the LEAs not covered in D3.3

Additional mitigations	Short description	Useful mitigation to prevent the following attack modes
Sectorization	The establishment of different security perimeters, with their corresponding filters and access control.	Vehicle used as a WEAPON, Package Type IED, Vehicle-borne IEDs (VBIEDs), Suicide bomb IED, CBRN attack, Shooting
Snipers	Allocate different sniper teams in strategic locations (e.g. potential attack areas).	Vehicle used as a WEAPON, Package Type IED, Vehicle-borne IEDs (VBIEDs), Suicide bomb IED, Shooting
Preventive control and surveillance	Establishment of security perimeters in the vulnerable zones object of the attacks.	Vehicle used as a WEAPON, Vehicle-borne IEDs (VBIEDs), Suicide bomb IED, CUTTING WEAPONS, Shooting
Video cameras and UAVs	When possible it would be useful to use video cameras and Unmanned Aerial Vehicles (UAV) located in places to monitor the event and detect suspicious signs and signals. The information would be useful for the command and control room to get a big picture of the situation.	Vehicle-borne IEDs (VBIEDs), Suicide bomb IED, CUTTING WEAPONS, Shooting

3.2 LEAS' INPUT FOR INNOVATIVE MITIGATIONS – WHAT IS STILL MISSING?

The second part of the template was thought to collect any input regarding measures that would be useful to improve current operations and ideas for new mitigations not available at the moment. Table 5 reports the main suggestions and ideas collected.

Table 3: Ideas for new mitigations not available at the moment

According to your experience, what is it still missing? Is there any new mitigation to be taken into account according to the specific attack mode? Please list and explain below.	Attack mode addressed
• **Design of perimeter closures for protecting the accesses** to the event venue under scientific criteria considering the rules of the evacuation plans and their possible impacts.	Vehicle used as a WEAPON (vehicle ramming) Shooting
• **Use of Automatic CCTV system** which is able to detect unusual driving (e.g. speeding, parking in suspicious areas).	Vehicle used as a WEAPON (vehicle ramming)
• **Protection services with Remotely Piloted Aircraft System (RPAs)** with on-board equipment with different technologies (sensors, cameras, etc.) capable of sending information about what is happening in sufficient detail to monitor the scenarios or places of protection. Drones would be a useful tool to support LEAs operations in detecting weak signals.	Vehicle used as a WEAPON (vehicle ramming) Package Type IED Vehicle-borne IEDs (VBIEDs) (Squad of) Suicide bomb IED CBRN attack Shooting

• **Tools for evaluating the impact of police actions**. It would be useful to have tools able to assess the degree of effectiveness of the measures used to mitigate the risks. In many cases, ineffective measures and even policies are implemented. It is also desirable to evaluate the efficiency of the policies, measures or tools used, cost-benefit analysis or the analysis of advantages and disadvantages in terms of discomfort, etc.	Vehicle used as a WEAPON (vehicle ramming) Vehicle-borne IEDs (VBIEDs) (Squad of) Suicide bomb IED Hijacking of social networks Shooting
• It would be useful to provide **training courses on detection techniques** and preventive approach offered to police forces and other stakeholders, namely Private Security and Soft targets security managers.	Package Type IED Vehicle-borne IEDs (VBIEDs) (Squad of) Suicide bomb IED CBRN attack Shooting
• **Improvement of technical equipment** for the detection of explosive. Some LEAs underlined that currently there are scanner systems that are not always operative and accessible from their own premises (e.g. Headquarters or district units).	Package Type IED
• **Use of portable and self-portable barrier systems**	Vehicle-borne IEDs (VBIEDs)
• **Communication actions countering fake news.** To mitigate the effect of fake news, LEAs in charge for the communication with the public should inform and publish the lack of truthfulness of given information, counteracting the message or encouraging critical thinking.	Hijacking of social networks
• Some of the LEAs highlighted that the use of social networks is currently under the competence of social media analysts and specialized sections (intelligence section). However, it would be useful to offer a **general awareness training course on the use of trusted Social Network channels** to a wider range of police officers. In general, this training is usually directed to social network analysts almost exclusively.	Hijacking of social networks

3.3 Mitigations for the additional attack modes included in D3.6

LEAs were also asked to describe the mitigations measures currently adopted to prevent the additional attack modes[3] identified in D3.6, namely:

- Drone based- attack;
- Hostages;
- Snipers;
- Aircraft used as weapon.

The main inputs collected from the experts are reported in Table 3[4]. It also comprises a specific section concerning ideas for future mitigation with respect to the additional attack modes.

[4] In this case, the table reports the feedback collected from 4 experts involved in the study, i.e. BayFHVR, EENA, ERT, LPV.

Table 4: Mitigations to address the additional attack modes included in D3.6

ADDITIONAL ATTACK MODES FROM D3.6	MITIGATIONS CURRENTLY IN PLACE WITHIN YOUR ORGANISATION OR FROM RESEARCH	DESCRIPTION OF THE MITIGATION	IDEAS FOR FUTURE MITIGATIONS
DRONE BASED ATTACK	**Apply regulation on the RPAs use**	Apply restrictions on the use of RPAs in specific sensitive areas.	The real challenge for the upcoming years is that Unmanned aircraft (or 'drones') is a fast developing sector of aviation and, even though drones are increasingly being used in the Europe Union, the regulatory framework is still fragmented. Although national safety rules have been established, these differ across the EU countries, and certain key safeguards are not addressed in a coherent way[5]. It would be important to test what are the most optimal counter-drone tools and procedures and prepare the legal framework that will regulate their use
	Surveillance of sensitive areas	Identification systems of RPAs and their owner. Sensitive areas are under surveillance by video or manually. The operator has to manually detect drones on the video. Currently, the Bavarian police (BayFHVR) are exploring automatic systems, but so far the automatic detection is not a standard procedure.	As underlined by BayFHVR, the automatic detection systems for drones are not working well enough at the moment. Especially if more than one drone arrives at the same spot at the same time. Normally tracing systems are focussing on one drone and then start to follow; if there are two or more the system can get confused.
	Constructional defence against drones	If possible, constructional defences systems like iron nets are used to secure buildings or event grounds against drones. Frequently this system is used in prisons in order to avoid drones	A wide range jamming of drones is technically nearly impossible at the moment, but it would be probably the best solution to be implemented.

[5] https://www.easa.europa.eu/easa-and-you/civil-drones-rpas

	smuggling drugs or weapons into the building. But, currently, the use of this is limited to buildings.	
Jamming of drones[6]	For open-air grounds with very sensitive security requirements, the use of jammers is possible. But the range of jammers application is limited.	
Hijacking technology	Hijacking technology is a “hacking the drone” method aiming to "capture" it and make it land.	
Geofencing	Geofencing is about defining no-fly zones based on coordinates. Drone manufacturers block the flying of their products in those areas. It is an option that works well in general and some manufacturers have already implemented it. While it is possible to geofence areas like airports, it is not easily possible to geofence all areas where a drone attack may take place and in the context of LETSCROWD areas where mass gathering events may be organised.	
Reactive detection, localization, inhibition and neutralization	Detection devices detect drones based on their signal and indicate the position of the pilot and the "home" return point of the drone. These devices only offer detection and they are good enough to detect threats, allowing locating the drone pilot and potentially stopping the drone. Currently, as reported by one of the expert, there is no a comprehensive solution that successfully covers all the four actions described.	

[6] Jamming specifically refers to intentionally using a transmission blocking signal to disrupt communications between a drone and the pilot https://www.dedrone.com/blog/primer-jamming-spoofing-and-electronic-interruption-of-a-drone

	Snipers against drones (shoot it down)	During events with high security risk (e.g. political summits), snipers have order to shoot unidentified drones down. But, depending on the location and the position of the drone, this is sometimes impossible without endangering other people. The "shoot it down" technique is a method of literally physically stopping the aircraft. This could be shooting bullets, nets, or anything that will take down the drone. Different approaches are already available and are also being researched.	
	Engineering anti drone system (e.g. the "Gladiator" in Antwerp)	It is a tool[7] that can shoot a net on to the enemy drone. The net takes the drone out and brings it to the ground, without damaging the drone.	
	Eagles	Eagles are used to pick enemy drones out of the air (e.g. used by the police in the Netherlands).	

ADDITIONAL ATTACK MODES FROM D3.6	**MITIGATIONS CURRENTLY IN PLACE WITHIN YOUR ORGANISATION OR FROM RESEARCH**	**DESCRIPTION OF THE MITIGATION**	**IDEAS FOR FUTURE MITIGATIONS**
Hostages	**Counter-Terrorism unit/ Training of police/ Better equipment**	Special counter terrorism units, as well as normal police officers, are regularly trained in hostage rescue. Also specialised negotiating groups are trained to speak with hostage-takers. There are internal regulations about the training of negotiator as well as clear protocol under which conditions a rescue should be attempted. Additionally the equipment has been improved during the last decade. New	

[7] See – as example - https://www.youtube.com/watch?v=CxeESBPBOSg

		bulletproof vests, helmets and weapons have been bought in order to improve the capacity of the police to deal with this situation.	
	Private Security Officers/ Sky marshals in aircrafts	For exposed targets, special measures (e.g. private security providers) or special trained sky marshals can be used. In the private sphere, where most of the kidnappings take place, these measures are useless.	
	Constructional measures at exposed buildings or other potential targets	Similar to the private security measures, exposed targets can be also secured by constructional measures - e.g. planes through a bomb-proof cockpit door or banks by using bomb-proof glass cabins for employees.	
	Personal protection of people susceptible to being kidnapped or threatened	Personal escort and/ or technological means of surveillance and protection can be used for this purpose.	Intelligence services with advanced information gathering system (e.g. artificial Intelligence), web monitoring, communications, localization and early detection of threats.
	Negotiation	Officers trained in negotiation.	Technology to protect agents in assaults and clean-ups in the face of armed threats.

ADDITIONAL ATTACK MODES FROM D3.6	MITIGATIONS CURRENTLY IN PLACE WITHIN YOUR ORGANISATION OR FROM RESEARCH	DESCRIPTION OF THE MITIGATION	IDEAS FOR FUTURE MITIGATIONS
Sniper	**Policies and regulations regulating long and war weapons**	Carry out administrative inspection of long and war weapons.	Intelligence services with advanced information gathering system (Artificial Intelligence), web monitoring, communications, localization and early detection of threats.
	Video surveillance	Snipers can be detected by using video surveillance. Operators can	Automatic detection systems that are able to detect suspicious

	inspect the environment of an event and take measures if they find something suspicious (e.g. like a person on a roof in a "red zone").	behaviour (e.g. at the airport) would be very helpful.
Access controls	Access controls with body scanners or metal detectors are a standard procedure for sensitive events. For large events (e.g. concerts, sport events, etc.) at least the bags are checked at the entrance.	
Securing neighbouring buildings before an event	In the case of large inner city events, like political demonstrations or public speeches of high-level persons with a high risk, the neighbouring buildings are checked. The people living there, are asked e.g. to keep their windows closed, etc.	
Detect the location and installing perimeters	The location of the event should be detected to check where it could be easy for a sniper to hide. The approach routes have to be planned accordingly, taking into account the possible locations for a sniper to hide.	
Strict weapon laws	A strict weapon law reduces the threat created by the private use of weapons, as well as it reduces the risk of rampage or assassination by snipers.	
Police Snipers	As a counter measure against snipers, also police snipers are used to neutralise potential aggressors. Analysis of specific risks against snipers, and planning of neutralization and mitigation devices.	
RECCE teams and information teams	A recce-team could be involved first, to detect possible snipers. At the same time, an intelligence	

		team is necessary to gather all the available information (e.g. social and other media that might be sending information about possible attacks).	
	Bullet proof "briefcases"	They look like briefcases and can be carried by the close protection team. If the sniper was not detected early enough, this item could help to protect the VIP.	
	Bullet proof vehicles and bullet proof vests	They allow lessening the shooter's efficacy, decreasing the possibility to hit the VIP.	

ADDITIONAL ATTACK MODES FROM D3.6	MITIGATIONS CURRENTLY IN PLACE WITHIN YOUR ORGANISATION OR FROM RESEARCH	DESCRIPTION OF THE MITIGATION	IDEAS FOR FUTURE MITIGATIONS
Aircraft used as a weapon	**Aviation regulations**	Restrictions of the flight areas	
	Surveillance of airspace and certain sensitive areas	Identification systems of aircraft and their owners	
	Constructional defence of exposed buildings	Endangered buildings like nuclear power plants have been secured against plane attacks according to a governmental plan started as a consequence of the 9/11 attacks.	Automatic detection systems that are able to detect suspicious behaviour (e.g. at the airport) would be very helpful.
	Change in law/ procedures of the military	As another consequence of 9/11, the law and the guideline for the use of the German air force was changed. In the case of the hijacking of a plane, the air force is allowed to bring down the plane, if the use as a weapon is clear, and all other measures (like evacuation of the target) are	

		not possible.
	Sky marshals	Special trained sky marshals are deployed in plane to avoid hijacking.
	Security measures at the airport	The security measures at the airport are high to prevent the use of weapons. Also analytical computer systems are used at the airport in order to identify potentially dangerous persons. Police officers and private security staff have a special training to identify signs of nervousness.
	Construction of the aircraft	Special security measures (e.g. bomb-proof cockpit door) difficult the hijacking of a plane.
	Data sharing about passengers / terrorists	International sharing of data between airlines, police and intelligence to identify suspects or persons with a terror background in order to prevent them from entering a plane.
	Direct line off contact with air traffic control	It allows having very fast information if a plane would be diverting from its original course. Through a direct line, the commander in chief will have more time to react to this information.

4 Mitigations resulting from the Letscrowd project: an update

This section reports an update of possible mitigation actions linked to the LETSCROWD outcomes developed within the project that could contribute to the prevention and minimization of the security threats described in D3.2 and D3.6.

While the majority of LETSCROWD outcomes could be potentially used to prevent specific terrorist attacks (Table 5), the Dynamic Risk Assessment (DRA) and the Innovative communication procedures (ICP), as methodologies, are transversal to the different terroristic attacks and would apply to all of them.

Dynamic Risk Assessment (DRA) as a tool to increase the situational awareness of the operator in charge of the security of a mass-gathering event becomes, *per se*, a mitigation measure for all attack modes identified in Deliverable D3.6 - Section 2.2, through the acquisition, processing and correlation of attack-specific weak signals (see the precursors identified in D3.6 - Section 2.2 - Table 3). Clearly, the higher the quality of the received weak signals and the precision of the rules to combine them, the bigger would be the mitigation potential. The discussion about the credibility of the sensors, reliability of the technologies in charge of detecting the weak signals and the rules to combine and correlate weak signals identified by the LEAs can be found in Deliverable D3.6, Sections 4 and 5.

The Innovative Communication procedures (ICP) was thought to be a tool to enhance event organisers, security officers and first responders' crowd awareness and communication competences in the pre-event phase and execution phase of a mass gathering event. The communication toolkit provides the users with some useful indications and recommendations to plan and improve the effectiveness of the communication strategies, the messages to be issued during critical situations and crowd behaviours to be fostered both in routine as well as critical situations. Therefore, the communication guidelines cannot be used to mitigate the effect of a specific attack mode, but rather as general recommendations to be aware of when organising mass gatherings.

As done in D3.3, the table below also reports suggestions from the technology providers' point of view regarding mitigations resulting from future research (when available).

Table 5: Update on mitigations coming from LETSCROWD

Attack mode	Description of the LETSCROWD mitigations	Suggestions for future research
Vehicle used as weapon (vehicle ramming)	***Crowd Modelling Tool***[8] (D5.1-M12 and D5.5 – M24). The work on the simulation of crowd behaviour and evacuation flow could help for a better location of the barriers, both to protect the crowd and to allow an easy evacuation even in presence of barriers. The same would be applied for the identification of the vehicle exclusion zones.	• Remote disabling of vehicles in a secure zone, access to vehicle tracking for security purposes[9] [10]

[8] For almost all the security threats discussed, the crowd modelling tool (including GIS technology, and evacuation alongside the RTE real-time evacuation tool) can be used to simulate the impact those may have on the crowd movement located in a specific place, plan for and optimise proposed mitigations (arisen from SRA) and, finally, re-test consequences after that risk mitigation have been applied.

[9] https://www.wired.com/story/phantom-teleops/

[10] https://purplegriffon.com/blog/carhacked-9-terrifying-ways-hackers-can-control-your-car

	Human-Centred Computer vision tools. They can help to detect vehicles, both parked in a suspect location and moving in/ close to the mass gathering venue. Existing methods for vehicle detection and tracking are currently focused on traffic monitoring. Their effectiveness to scenarios of interest to LETSCROWD has to be verified yet.	
Package Type IED	***Crowd Modelling Tool*.** It can be used in the event preparation phase to simulate the impact a suspect package (unexploded IED) may have on the crowd movement in a given area of a mass gathering venue, but also the evacuation of the venue where an explosion may have blocked exit routes. This will help to identify mitigations by better planning exit routes, evacuation strategies and in staff training to better identify crowd movements if a suspect package has been placed in the venue, through the visualisation of the simulated crowds. ***LEAs training package*** (D7.6 - M26). LETSCROWD will develop a crowd protection-training package for enhancing the "human factor" capabilities as "security sensor". These capabilities also include identifying and recognizing suspicious activities of persons and identification of suspicious objects and vehicles, and providing guidelines of emergency responses to suspicious items and patterns identified in (5). ***Human-Centred Computer vision tools*** (D5.4 – M12 and D5.8 – M24). The image-based person re-identification tool can be used to search in the available videos for a person that abandoned an object, starting from images of this event seen by the operator. That person can be searched by the operator in the available videos to analyse his/her behaviour	• Incorporating stand-off distances (based on TNT equivalent) to current or future crowd and evacuation models. • A screening tool based on quantitative data and expert judgements could be designed for security managers to identify critical locations for IED attacks and prioritize resources allocation.
Vehicle-borne IEDs (VBIEDs)	***Crowd Modelling Tool.*** See above (package type). ***LEAs training package*.** See above (package type). ***Human-Centred Computer vision tools.*** *See above* (vehicle used as a weapon).	
(Squad of) Suicide bomb IED	***LEAs training package*; *Crowd Modelling Tool*; and *Human-Centred Computer vision tools***. LETSCROWD is studying crowd behaviours to help identify terrorists and suspicious behaviours, some of which could be	• Technologies that could detect explosives and/or metal from the distance[11]

[11] http://www.camero-tech.com/

	specific to suicide bombers. This can be through: • the training of the staff working at the mass gathering (not only security staff) to report behaviours, combined with public reporting. • the automated camera detection, where crowd simulations will forecast "normal" situations and be used to train the camera to detect "abnormal situations". The performance of existing computer vision methods for the detection of anomalous behaviour detection still need to be tested.	
CBRN attack	***Crowd Modelling Tool.*** The work on the simulation of crowd behaviour and evacuation flow could help the easy evacuation of public in the event CBRN attack has occurred.	• Forecasting of spillage/containment requirements and crowd management (6), 'pop up' decontamination tents[12].
Cold steel (e.g. stabbing)	***LEAs training package***. Thanks to LEAs' training and human behaviour investigation, officers will improve their ability and skills to detect anomalous human behaviour patterns which might indicate attack intention. ***Human-Centred Computer vision tools (e.g. crowd monitoring).*** Real time crowd behaviour forecast will allow a quick detection of unexpected or rare crowd movements through video analysis and computer vision. The performance of existing computer vision methods for the detection of anomalous behaviour detection still need to be tested.	• Technologies that could detect metal from the distance. • Portable walk through x ray detectors.
Hijacking of social networks	***Semantic intelligence*** applied to social networks and Web contents. It enables security analysts to assess threats for mass gathering event from the analysis of large text collections gathered from social networks and web sites in general.	***N.a***
Shooting	***Crowd Modelling Tool.*** The simulation of crowd behaviour and evacuation flow could help the easy evacuation of public in the event shooting attack has occurred. ***LEAs training package*** designed to enhance capabilities of police officers in identification of suspicious signs in behaviour and appearance. ***Semantic intelligence*** applied to social networks and	• Stochastic simulation of shooting attacks at mass gathering events. Most current models are deterministic and mainly oriented to reduce shooter capacity (armed resistance) or active shooter attacks at educational

[12] https://www.losberger.com/us/en_US/products/rapid-deployment-systems-us/

	Web contents acquired by a focused crawler. Web crawling engine might help LEAs to receive early warning and intelligence regarding the targeting of mass gathering events and actual preparations to organize attacks.	institutions. The future model be able to simulate the characteristics, decisions and actions of people involved (civilians and shooters) using Monte Carlo methods to capture stochastic variations in the outcomes. Faster than real-time simulations are desirable. The suggested outputs can be the number of casualties, the survival probability and the shooter effectiveness (7), (8), (9), (10).
Drone-based attack	***N.a***	• Technologies to send drone back to operator/base[13]
Hostages	***N.a***	• New viewing technologies that could provide visuals or video of images from behind walls
Sniper	***N.a***	***N.a***
Aircraft used as weapon	***N.a***	***N.a***

Finally, some new ideas were also suggested to improve crowd management and communications as follows:

1. Crowd management: Deployable inflatable crowd barriers[14], gamification for self-regulating crowd behaviour (11);
2. Communication: Single person mobile dynamic signs, active social identity psychological messaging (12).

4.1 Long-term mitigation measures to fight terrorism: partnerships, public advertising campaigns and trainings

As reported in (13), terrorism is as a global phenomenon and the terrorist methodologies are continuously evolving. Since 2015 the EU Parliament has approved a set of measures to address the threat of terrorism (14), some of them are synthetize as follows:

- EU additional funding budget for the fight against terrorism;
- Upgrade of the EU arms export control;

[13] https://www.apolloshield.com/

[14] https://landmarkcreations.com/inflatable-products-gallery/inflatable-pylons/item/crowd-barrier-l2418

- Creation of a special committee to tackle deficiencies in the fight against terrorism and propose improvements[15];
- Give Europol additional powers to helps member states fight terrorism. The new powers will allow the European agency to set up specialised units more easily in order to promptly respond to emerging threats[16].
- Proposals and strategies to prevent radicalisation to be applied in particular in prison, online and through educations and social inclusion[17]. In line with this, in 2018, the French government has promoted some communities terrorism prevention programmes especially addressed to young people. A national plan has been launched by the government as strategy to prevent the phenomenon of radicalisation[18].

One of the main challenges for the upcoming years would be to build **long-term partnerships** between public and private sectors (e.g. police forces, academia institutions and counter terrorism authorities) at national and European level to foster closer collaboration and cooperation, improving information sharing, training opportunities and knowledge exchange and experience of global terrorism threat. As reported in (15) to fight terrorism, it is essential to have optimal information exchange and accurate data. That is why, since 2007, Europol has published the EU Terrorism and Trend report in order to align national governments and police forces about the European situation on annual basis. In UK, a team of senior security officers founded the cross-sector safety and security communications (CSSC) initiative which aims to facilitate communications between private and public sectors on issues related to security[19] .

Furthermore, the National Terrorism Security office developed some guidance and short movies[20] for staff working in crowded places, showing them what to expect and how to respond to the terrorist threat. The main topics covered by the movies are the following:

- Identification and response to suspicious activity and behaviour;
- Identification of suspicious items;
- Reaction to firearms or weapons attacks;
- Introduction to counter terrorism awareness.

In general, the implementation and **delivery of initial and continuing security awareness training courses** for both practitioners and front-end operators working in crowded places and critical environments (e.g. transport hubs, hotels large arenas, cultural sites and shopping malls) would be an effective mitigation

[15] http://www.europarl.europa.eu/news/en/press-room/20170629IPR78658/special-committee-to-tackle-deficiencies-in-the-fight-against-terrorism

[16] http://www.europarl.europa.eu/news/en/headlines/security/20160509STO26397/fight-against-terrorism-parliament-approves-updated-powers-for-europol

[17] http://www.europarl.europa.eu/news/en/press-room/20151120IPR03612/ep-calls-for-joint-eu-strategy-to-fight-radicalisation-of-young-eu-citizens

[18] http://bourgogne-franche-comte.drdjscs.gouv.fr/spip.php?article1155

[19] https://www.thecssc.com/about/

[20] https://www.gov.uk/government/news/travel-industry-training-staff-to-deal-with-terrorist-incidents

measure to prevent terrorism. Indeed most of the time, front-end operators are typically the ones who are most likely to first identify and report a security threat[21].

The **development of a security culture involving communities** at national and local level would be another effective long-term action to defeat terrorism. Citizens and general public could play an important role in tackling terrorism[22], supporting the police forces in preventing terroristic attacks and saving lives. Recently, the National Counter Terrorism Security Office has launched several public campaigns and initiatives to raise awareness among citizens on terrorist attacks, namely:

- "**Look campaign**" is a defeat terrorism advertising campaign launched in cinemas[23] [24]. Cinemas were selected as effective place to:
  - deliver the message with fewer distractions;
  - be more effective;
  - reach different types of audience, usually difficult to reach as young people.
- **"Stay Safe film"** provides citizens with some useful advice on the steps they can take to keep themselves safe in the rare case of firearms or weapons attacks[25].The guidance provided could be applied to any place.
- **Reporting suspicious activity and behaviour[26]** is an initiative that aims at involving public to support police tackles terrorism and safe lives by reporting suspicious behaviours.

In line with, this the Belgian authorities launched a webpage "Risk-info.be" which aims to provide citizens with useful information on how to behave in case of terroristic attacks[27].

Despite not exhaustive, this paragraph has synthetized some of the current long-term actions undertaken at both European and National level to prevent the threat of terrorism.

[21] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/625594/CT_Awareness_-_Helpful_Advice_Leaflet.pdf

[22] http://www.guernsey.police.uk/ACT

[23] https://www.gov.uk/government/news/new-communities-defeat-terrorism-campaign-launched

[24] https://www.npcc.police.uk/NPCCBusinessAreas/WeaponAttacksStaySafe.aspx

[25] https://www.gov.uk/government/publications/stay-safe-film

[26] https://www.gov.uk/government/news/action-counters-terrorism-report-suspicious-activity-and-behaviour

[27] https://www.info-risques.be/fr

5 Conclusions

The two versions of deliverables on soft and hard mitigation measures (D3.3 and D3.7) have reported an extensive overview of the mitigation measures currently available and adopted by the European police forces to tackle terrorism.

A study involving seven senior police officers from LEAs participating in the LETSCROWD project was carried out in order to enrich and integrate the main findings came out from the literature review in D3.3. LEAs contribution was fundamental to report the expert point of view.

LEAs were mainly asked to indicate the current and potential mitigations to prevent the following threats:

- Vehicle used as weapon (vehicle ramming)
- Package Type IED
- Vehicle-borne IEDs (VBIEDs)
- (Squad of) Suicide bomb IED
- CBRN attack
- Cold steel (e.g. stabbing)
- Hijacking of social networks
- Shooting
- Drone based- attack
- Hostages
- Snipers
- Aircraft used as weapon

The qualitative study conducted within D3.7 aimed to: 1. identify the mitigation measures currently applied by the Law Enforcement agencies to address the attack modes identified in D3.2 and updated in D3.6; and 2. collect any input regarding measures that would be useful to improve current operations and ideas for new mitigations not available at the moment.

In general, most of the LEAs reported that: 1. automatic detection systems able to detect suspicious behaviours; 2. improvement of technical equipment currently available; and 3. the implementation of awareness training courses on different subjects (e.g. detection techniques and use of trusted social network channels) offered to police forces and other key relevant stakeholders would be useful solutions to improve current operations.

6 REFERENCES AND ACRONYMS

6.1 References

1. **LETS-CROWD project.** *"Deliverable D3.3 Progress report on soft and hard mitigations".* 2018.

2. **LETS-CROWD project.** *"Deliverable D3.6 Dynamic risks for mass gatherings".* 2018.

3. **LETS-CROWD project. .** *Deliverable D3.2 LETSCROWD Progress report on dynamic risks for mass gatherings.* 2018.

4. **LETS-CROWD project.** *"Report on training package for crowd protection based on human factor".* 2018.

5. **LETS-CROWD project.** *Deliverable 3.1 Progress report on models of patterns of human behaviours.* 2017.

6. *Advanced integrative multiscale modeling system for countering the threat of CBRN terrorism.* **Yee, E., & Hogue, R.** s.l. : In Proceedings of NATO Modeling and Simulation Group Conference , 2008.

7. *Mitigating Active Shooter Impact; Analysis for Policy Options Based on Agent/Computer Based Modeling.* **Anklam, C. et al.** DOI: 10.5055/jem.2015.0234., s.l. : Journal of Emergency Management, 2014, Vol. 13(3).

8. *Active Shooter: An Agent-Based Model for Unarmed Resistance.* **Briggs, T.W. & Kennedy, W.G.** IEEE Press. 3521-3531., s.l. : Proceedings of the 2016 Winter Simulation Conference., 2016.

9. *Agent-based simulation of mass shootings: Determining how to limit the scale of a tragedy. .* **Hayes, R., & Hayes, R.** 1-12, s.l. : Jasss-the Journal of Artificial Societies and Social Simulation, 2014, Vol. 17(2).

10. **Steward, A.** Active shooter simulations: An agent-based model of civilian response strategy. [Online] 2017. https://www.imse.iastate.edu/files/2014/03/StewartAlex-thesis.pdf.

11. *'Gamification': Influencing health behaviours with games.* **King, D., Greaves, F., Exeter, C. and Darzi, A.** 2013.

12. *'Keeping the Peace' Social Identity, Procedural Justice and the Policing of Football Crowds.* **Stott, C., Hoggett, J. and Pearson, G.** s.l. : The British Journal of Criminology, 2011, Vol. 52(2).

13. **Centre, Pool Re's Terrorism Research and Analysis.** Terrorism Threat & Mitigation Report. [Online] 2017. https://www.nsr-org.no/getfile.php/139676-1506512168/Dokumenter/Eksterne%20publikasjoner/Pool-Re-Terrorism-Threat-Mitigation-Report-TMR-2-17.pdf.

14. **European Parliamentary Research Service, Europol.** http://www.europarl.europa.eu/infographic/europe-and-terrorism/index_en.html . [Online]

15. **Europol.** *EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT 2018 (TESAT).*

6.2 Acronyms

Acronyms List	
CBRN	Chemical, biological, radiological, and nuclear
CMP	Crowd Modelling and Planning tool
CPTED	Crime Prevention through environmental design
DRA	Dynamic Risk Assessment
GIS	Geographic Information System
HCV	Human-Centred Computer Vision
ICP	Innovative Communication Procedures
IEDs	Improvised explosive devices
LEA	Law Enforcement Agency
LTP	LEA Training Package
PMT	Policy Making Toolkit
SIE	Semantic Intelligence Engine
SNs	Social Networks
SVBIED	Suicide Vehicle Borne Improvised Explosive Device
VBIED	Vehicle Borne Improvised Explosive Device
WTMD	Walkthrough metal detector

7 ANNEX A

7.1 Synthesis of the mitigation actions from D3.3

Type of Attack Mode (From D3.2)	Existing mitigation measures from the literature review	Short description of the mitigation measure form D3.3
1. Vehicle – ramming attack	*1.1 Barriers and creation of vehicle exclusion zones*	Barriers are probably the primary way to mitigate vehicle-ramming attacks. Barriers can be built around vulnerable crowded areas, often as permanent or temporary bollards. The US state department "anti-ram vehicle list" lists several types of bollards to protect the perimeter of its embassies abroad. Measures can also include tight bends and restricted-width streets to prevent a large vehicle building speed before reaching a bollard or barrier. Similar measures can be used to oblige vehicles to maintain a limited speed.
	1.2 Sensitize and Training for detection of weak signals	A proper sensitization and training of the operators of the commercial vehicle industry, of the car rental staff and of the general public to be vigilant and report about indicators can represent an effective way to help preventing ramming attacks.
	1.3 Control on vehicle rental and operation	A possible mitigation action regarding the risk of a vehicle –ramming attack should focus on the procurement of the vehicle used for the ramming attack. The large majority of these attacks were perpetrated using rented or stolen vehicles. The mitigation should focus on this specific phase of the attack preparation.
2. Package type IED	*2.1 Counter – IEDs awareness and training in suspicious behaviours*	Training courses to build counter-IED capabilities, enhance awareness of IED threats, be alert for suspicious behaviour and IED indicators are the most common and effective defence to reduce risk of IED threats. Several governmental services (e.g. TRIPwire – U.S. Department of Homeland Security) provide training programmes addressed to stakeholders that could be involved in IEDs identification or concerned about them (e.g. critical infrastructures

		owners and operators; event organizer staff).
	2.2 Explosive detection system	The detection of IEDs presents a real challenge for all the stakeholders involved in their identification (e.g. security screeners, employees, first responders, military personnel), especially in case of outdoor events and without ingress control (e.g. Boston Marathon Bombing, 15/4/2013). Several bomb detection technologies have been developed for their employment in critical zones or in high-risk events. These include "trace detectors" for identifying trace amounts of commonly used explosive in the air; millimetre-wave technology" to detect dense objects hidden under clothes. Also explosive-detection dogs are usually used to identify and locate chemical explosive used in many different critical scenarios.
3. Vehicle – borne IEDs (VBIEDs)	*3.1 Counter – IEDs awareness and training in suspicious behaviours*	Training courses to build counter-IED capabilities, enhance awareness of IED threats, be alert for suspicious behaviour and IED indicators are the most common and effective defence to reduce risk of IED threats. Several governmental services (e.g. TRIPwire – U.S. Department of Homeland Security) provide training programmes addressed to stakeholders that could be involved in IEDs identification or concerned about them (e.g. critical infrastructures owners and operators; event organizer staff).
	3.2 Vehicle surveillance and control/ inspection	The countermeasures to address VBIEDs attacks include vehicle surveillance and control/ inspection. The first stage of the process consists in the surveillance of all vehicles entering the close public roadways leading to event venue. Then, it is important to control and assess of all vehicles on the approach roads.
	3.3 Anti-ram vehicle barriers	Since the stand-off distance is the most important factor in determining the extent of damage for a given-size VBIEDs (each additional increment of stand-off provides progressively more protection), achieving anti-ram setback is an effective blast mitigation measure for this type of attack (1). They can be used to

		protect the perimeters of the site where the mass-gathering event takes place, creating vehicle exclusion zones. Especially, in case of an event is hosted in a specific building/ infrastructure (e.g. stadium, concert hall, etc.) or in a venue surrounded by buildings (e.g. a square), specific stand-off measures could be estimated with regards to these ones.
4. (Squad of) Suicide bomb IED	*4.1 Counter – IEDs awareness and training in suspicious behaviours*	Training courses to build counter-IED capabilities, enhance awareness of IED threats, be alert for suspicious behaviour and IED indicators are the most common and effective defence to reduce risk of IED threats. Several governmental services (e.g. TRIPwire – U.S. Department of Homeland Security) provide training programmes addressed to stakeholders that could be involved in IEDs identification or concerned about them (e.g. critical infrastructures owners and operators; event organizer staff).
	4.2 Physical barriers	Barriers can be built around vulnerable crowded areas for mass gatherings planned in advance, especially those that are ticketed or have a limited capacity. "External barriers or a strengthened perimeter to prevent a penetrative (ramming) or close proximity (parked or encroachment) attack" are recommended in (1).Essentially, this means creating a perimeter that dissuades or makes it difficult or impossible for a potential suicide bomber to get close to crowds in the mass gathering without passing security.
	4.3 Security and Id Checks	Procedures similar to security control at airports are common at mass gathering events such as the Olympics. These involve the use of a magnetic scan (handheld or through an archway) and a search of any bag visitors have on their person (manual by security staff or through x ray machine). They can also involve sniffer dogs that will identify explosives on a person. Similarly, a person's ID can be checked on entry – either through tickets, or registering anyone's attendance. This is possible when a perimeter has been set up as above, allowing potential terrorists to be identified and bombs to be detected.

	4.4 Sniffer Dogs	Sniffer dogs are capable of detecting explosives and can be used to identify a person carrying a suicide bomb. Ad hoc checks around the event with sniffer dogs, and random searches can be carried out in place of the security checks for open events or as well as.
5. CBRN Attack	*5.1 Chemical agents detectors*	Chemical detection is performed by clinic tests on effected persons and air sampling intended to provide early warning available only in very specific scenarios mostly when the material is spread in an open space and moved by a wind. Detection of Chemical Warfare agents (CWA) and Toxic Industrial Chemicals (TIC) is relatively in the most advanced stage of development (comparing to other CBRN threats) and widely used in many key locations guarding the public against terror attacks and chemical spills. The existing chemical detection systems are expensive and incomplete regarding the full range of chemical threats however, they play a crucial role in "early warning" and possible minimizing the casualties if the facility is properly prepared for professional response. Detection technologies can be grouped into three major categories: point detection, standoff detection, and analytical instruments [40].
	5.2 Training for detection of possible attacks	Since chemical attacks are extremely difficult to prevent one of the most practical ways to mitigate the consequences of the attacks is to train and educate police officer and other field agents/employees to identify the possible indications that CBRN terror attack has occurred.
6. Cold steel	6.1 Security checks and metal detectors at the event entrances	The security controls and checks at event entry points will allow the Police to check people entering the event and metal detectors will be placed for the bags checking.
7. Hijacking of social networks	7.1 Improve the security access to Social Networks	This measure can reduce the risk of compromised accounts through the protection of social media platforms, sites and accounts at the technical or system level.

	7.2 Creating awareness on the use of trusted Social Networks	This mitigation measure will support the LEAs and event organisers in disseminating, together with the event dissemination material, the links to the official social networks channels used.
8. Shooting Attack	8.1 Body search	Body search (tapping) is one of the most efficient techniques for detection of concealed weapons. This method is widely used in events such as football games and concerts. The method could be only applied in closed venues where access points are controlled by security staff. When applying this technique the security staff must separate the belonging of the visitors for further inspection (done manually or using scanning machines).
	8.2 Walkthrough metal detector (WTMD)	Walkthrough metal detectors are wildly used for numerous security applications including screening of people in airports, train stations, shopping malls, etc. They detect metallic objects on people passing through the detector. Most WTMD are available with different numbers of detection zones, i.e. 1, 2, 6, 12, 18 and 33 zones, the greater number of detection's zones the more accurate the location of metallic object on the person can be determined, saving operator time. The level of detection sensitivity can be adjusted to meet varying threats.
	8.3 X-ray scanning machine	X-ray machines are used to scan luggage of people in controlled access points. They are widely used in various applications such as airports, train stations, sporting venues, exhibitions, shopping malls, seaports and other secure facilities. Typical application requires using them in closed venues with limited number of access points.
	8.4 Training for identification of suspicious signs in behaviour and appearance	Empirical research and lessons learned from past terror attacks shows that prior to terror attacks threat indications can be identified by trained personnel enabling them to report suspicious activity or take immediate action to stop the attack (1).

7.2 Excel template

ID	ATTACK MODE identified in D3.2	WHICH MITIGATION STRATEGIES DO YOU CURRENTLY APPLY TO ADDRESS THE SPECIFIC ATTACK MODE?					NEW AND INNOVATIVE MITIGATIONS
		1. BELOW THE MITIGATIONS IDENTIFIED THROUGH THE LITERATURE REVIEW IN D3.3, *PLEASE SELECT THOSE CURRENTLY USED BY YOUR ORGANISATION, IF ANY.* *(For a detailed description of each mitigation please refer to D3.3)*		2. PLEASE USE THIS COLUMN TO EXPLAIN WHY YOU DIDN'T SELECT A SPECIFIC MITIGATION (E.G. NOT APPLICABLE IN MY ORGANISATION, TOO EXPENSIVE, ETC.)	3. PLEASE LIST BELOW OTHER MITIGATIONS NOT IDENTIFIED YET, BUT CURRENTLY USED BY YOUR ORGANISATION	4. PLEASE, INCLUDE A SHORT DESCRIPTION OF EACH MITIGATION YOU LISTED IN THE PREVIOUS COLUMN	5. ACCORDING TO YOUR EXPERIENCE, WHAT IS IT STILL MISSING? ARE THERE ANY NEW MITIGATIONS TO BE TAKEN INTO ACCOUNT ACCORDING TO THE SPECIFIC ATTACK MODE? PLEASE LIST AND EXPLAIN BELOW.
1	**Vehicle used as a WEAPON (vehicle ramming)**	Barriers and creation of vehicle exclusion zones	X				
		Sensitisation and training for detection of weak signals					
		Control on vehicle rental and operation					
2	**Package Type IED**	Counter – IEDs awareness and training in suspicious behaviours					
		Explosive detection systems					
3	**Vehicle-borne IEDs (VBIEDs)**	Counter – IEDs awareness and training in suspicious behaviours					
		Vehicle surveillance and control/ inspection					
		Anti-ram vehicle barriers					
4	**(Squad of) Suicide bomb IED**	Counter – IEDs awareness and training in suspicious behaviours					
		Physical barriers					
		Security and ID Checks					
		Sniffer dogs					
5	**CBRN attack**	Chemical agents detectors					
		Training for detection of possible attacks					
6	**CUTTING WEAPONS - Cold steel (e.g. stabbing)**	Security Check at the event entrances					
		Security Officers inside the Mass					
		Setting major security measures along the venue perimeters					
7	**Hijacking of social networks**	Improving the security of access to SNs					
		Creating awareness on the use of trusted SN channels					
		Identifying trusted channels for cultural minorities					
		Counteract the spread of misinformation					
		Mitigating the Crowd-turfing by the use of automated crawling systems that are able to identify fake messages					
8	**Shooting**	Body search					
		Walkthrough metal detector (WTMD)					
		X-ray scanning machine					
		Training for identification of suspicious signs in behaviour and appearance					

Figure 9: Screenshot of the excel template