



Title:	Document Version:
D3.3 Progress report on hard and soft mitigations	1.00

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*:
M11 (March 2018)	M11 (March 2018)	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:
Alberto Pasquini	Deep Blue	WP3

Authors (organisation):

A. Pasquini, A. Golfetti, S. Giorgi (Deep Blue); P. Townsend (CROWD); A. Ruiz Temina (ETRA); C. Dambra (PROPRS); Y. Alon, C. Graf (RAILSEC); A. Cuesta (UC)

Abstract:

This document is the first version of the report on soft and hard mitigation measures. It identifies and describes soft and hard mitigations usable to mitigate the vulnerabilities and threats identified in Task 3.2 and reported in D3.2. It will be the basis for the deliverable D3.7.

Keywords:

Mass gathering, risk management, risk treatment, mitigations, effects on frequency and severity, security threats

Revision History

Revision	Date	Description	Author (Organisation)
V0.1	15.02.2018	D3.3 Table of Content	A. Pasquini (DBL)
V0.02	21.02.2018	Revised D3.3 ToC	A. Pasquini (DBL)
V0.03	07.03.2018	First contributions	Y. Alon, C. Graf (RAILSEC); C. Dambra (PROPRS); P. Townsend (CROWD); A. Ruiz Temina (ETRA)
V0.04	20.03.2018	Full draft	A. Pasquini, A. Golfetti, S.Giorgi (DBL)
V0.03	26.03.2018	Version with comments from internal review (UC and RAILSEC)	A. Pasquini, A. Golfetti, S.Giorgi (DBL); Y. Alon, C. Graf (RAILSEC); Arturo Cuesta (UC)
V1.00	29.03.2018	Final version ready to be submitted to EC	A. Pasquini, 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

The work described in this document has been conducted within the LETSCROWD project. This document reflects only the LETSCROWD Consortium view and the European Union is not responsible for any use that may be made of the information it contains.

This document and its content are the property of the LETSCROWD Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the LETSCROWD Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the LETSCROWD Partners.

Each LETSCROWD Partner may use this document in conformity with the LETSCROWD Consortium Grant Agreement provisions.

Executive Summary

This document represents a first version of the soft and hard mitigations actions for the security threats identified in D3.2 “Progress report on dynamic risks for mass gatherings” [1].

The deliverable is structured around the 4 main sections as follows:

1. **Section 2**, the theory of the risk treatment have been discussed according to the risk management process (standard ISO 31000) and including specific stages concerning the identification, selection, prioritization and planning of mitigation actions. Different types of mitigations have been specified: Crime Prevention through environmental design - CPTED¹ (hard), organizational actions (soft), and actions based on personnel and related training (soft).
2. **Section 3**, possible mitigations have been described according to the main risks identified in D3.2 [1]. The mitigation actions are presented including:
 - a short description of the risk;
 - a description of the reasonable worst-case scenario based on literature;
 - a description of the possible existing mitigation actions by detailing:
 - the possible effects on frequency and severity;
 - the potential adverse effects;
 - the stakeholders responsible for implementing the mitigation action.

Mitigations are not universal and shall be selected on the basis of the characteristics of the event under analysis 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. That's why only generic information is provided for each mitigation, together with an extensive bibliography. Other mitigation actions come out from the work carried out in LETSCROWD have been included. They consist of contributions that the project can provide to prevent the different terrorism attack modes² including project technological solutions (e.g. tools like: crowd modelling, semantic intelligence, human computer vision, policy making toolkit) and methodologies (e.g. dynamic risk assessment). The mitigations proposed both from the literature review and from the LETSCROWD project refer to the event preparation phase (i.e. early planning and pre-event).

3. **Section 4** reports conclusions and next steps. The second version of the deliverable (D3.7) will collect LEAs' mitigation strategies, needs and gaps and explore possible mitigation actions concerning hazards generated by the crowd as a consequence of a security threat (possible cascade effects).

¹ <http://www.popcenter.org/tools/cpted/PDFs/NCPC.pdf>

² Even if this deliverable mainly addresses security threats related to different terrorism attack modes, LETSCROWD also covers criminal actions (riots, demonstrations, disturbances, etc.).

Index

1	INTRODUCTION	7
1.1	PURPOSE OF THE DOCUMENT	7
1.2	SCOPE OF THE DOCUMENT	7
1.3	STRUCTURE OF THE DOCUMENT	7
2	THEORY OF RISK TREATMENT	8
2.1	RISK MANAGEMENT	8
2.2	RISK TREATMENT: MITIGATION MEASURES	9
2.2.1	IDENTIFICATION OF POSSIBLE MITIGATION ACTIONS	10
2.2.2	AVOIDANCE	10
2.2.3	REMOVING THE RISK OR REDUCING ITS PROBABILITY	10
2.2.4	REDUCE THE SEVERITY OF THE CONSEQUENCES	11
2.2.5	TYPES OF MITIGATION ACTIONS	11
2.3	SELECTION AND PRIORITIZATION OF MITIGATION ACTIONS	12
2.4	PLANNING OF THE MITIGATION ACTIONS	14
3	MAIN RISKS IDENTIFIED IN LETSCROWD AND POSSIBLE MITIGATION ACTIONS	14
3.1	MITIGATION ACTIONS: STRUCTURE AND COMPONENTS	17
3.2	VEHICLE-RAMMING ATTACK	17
3.2.1	DESCRIPTION OF THE RISK	17
3.2.2	REASONABLE WORST-CASE SCENARIO	18
3.2.3	POSSIBLE EXISTING MITIGATION ACTIONS	18
3.3	IMPROVISED EXPLOSIVE DEVICES (IEDs)	21
3.3.1	DESCRIPTION OF THE RISK	21
3.3.2	REASONABLE WORST-CASE SCENARIO	23
3.3.3	POSSIBLE EXISTING MITIGATIONS COMMON TO THE THREE TYPES OF IED ATTACKS	25
3.3.4	PACKAGE TYPE IED: SPECIFIC MITIGATION ACTIONS	26
3.3.5	VEHICLE-BORNE IEDs (VBIEDs): SPECIFIC MITIGATION ACTIONS	27
3.3.6	(SQUAD OF) SUICIDE BOMBER (S): SPECIFIC MITIGATION ACTIONS	29
3.4	CBRN ATTACK	30
3.4.1	DESCRIPTION OF THE RISK	30
3.4.2	REASONABLE WORST-CASE SCENARIO	31
3.4.3	POSSIBLE EXISTING MITIGATIONS	32
3.5	COLD STEEL	33
3.5.1	DESCRIPTION OF THE RISK	33
3.5.2	REASONABLE WORST-CASE SCENARIO	34
3.5.3	POSSIBLE EXISTING MITIGATIONS	34
3.6	HIJACKING OF SOCIAL NETWORKS	35
3.6.1	DESCRIPTION OF THE RISK	35
3.6.2	REASONABLE WORST-CASE SCENARIO	36
3.6.3	POSSIBLE EXISTING MITIGATIONS	37
3.7	SHOOTING ATTACK	38

3.7.1	DESCRIPTION OF THE RISK	38
3.7.2	REASONABLE WORST-CASE SCENARIO	39
3.7.3	POSSIBLE EXISTING MITIGATIONS	39
3.8	POSSIBLE ADDITIONAL MITIGATIONS RESULTING FROM THE WORK IN LETSCROWD AND RESEARCH	42
4	CONCLUSIONS AND NEXT STEPS	46
5	REFERENCES AND ACRONYMS	47
5.1	REFERENCES	47
5.2	ACRONYMS	51

LIST OF FIGURES

Figure 1: Risk management process with a focus on risk treatment	8
Figure 2: Elements affecting mitigation selection	13
Figure 3: The Static & Dynamic Risk Assessment stages (from D3.2)	15
Figure 4 - Explosive evacuation distance according to the different IEDs types.....	22

LIST OF TABLES

Table 1: List of hazards presented by the crowd and by the venue (from D3.2)	15
Table 2: List of risks related to terrorism and the proposed mitigations.....	16
Table 3: Mapping among LETSCROWD contributions, risk assessment stages and attack modes	42
Table 4: Possible additional mitigations resulting from LETSCROWD and research	43

1 INTRODUCTION

1.1 PURPOSE OF THE DOCUMENT

WP3 aims to provide security practitioners with an extension of the European Security Model (ESM). Four main tasks compose the WP3, as follows:

- *Task 3.1 Modelling of patterns of human behaviours.* The task aims at identifying a list of suspicious patterns that could be potentially interpreted as triggers of threats or hazards;
- *Task 3.2 Analysis of dynamic risks,* defines the methodology to dynamically assess the risks for crowds during mass gathering events;
- *Task 3.3 Soft and hard mitigation solutions,* select soft and hard solutions usable to mitigate vulnerabilities and threats identified in T3.2;
- *Task 3.4 ESM Implementation based on dynamic risk assessment,* combines results of tasks 3.1, 3.2 and 3.3 to produce the dynamic risk assessment methodology, integrating the static approach with the dynamic assessment of the risks.

This document is the first version of the soft and hard mitigation measures identified within T3.3. It describes soft and hard mitigations actions related to the security risks reported in D3.2 [1] and identified in T3.2.

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 in Task 3.2 and reported in D3.2 [1].

The main objectives of the document can be summarised as follows:

- to introduce the risk treatment process;
- to describe the existing soft and hard mitigation measures including the possible effects on frequency and severity; the potential adverse effects and the stakeholders responsible for implementing the mitigation action;
- to suggest possible mitigation actions coming out from the work carried out in LETSCROWD to be further developed in the second version of the deliverable D3.7.

1.3 STRUCTURE OF THE DOCUMENT

The document is organized in 3 main sections:

- Section 2 describes the theory of the risk treatment according to the standard ISO31000, also introducing other aspects related to the LETSCROWD project. It describes how mitigation actions can be used for reducing the probability of the risk and the severity of the consequences;
- Section 3 is dedicated to identify and describe possible mitigation actions for the risks that could occur in a mass-gathering event and that have been identified in LETSCROWD;
- Section 4 reports conclusions and next steps.

2 THEORY OF RISK TREATMENT

2.1 RISK MANAGEMENT

The **Risk management** is the process operating on the risks associated to an event. According to ISO31000, it can be defined as the: *“Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk”* [2].

Figure 1 summarizes the risk management process, including its main phases and typical components, and aspects related to the LETSCROWD project.

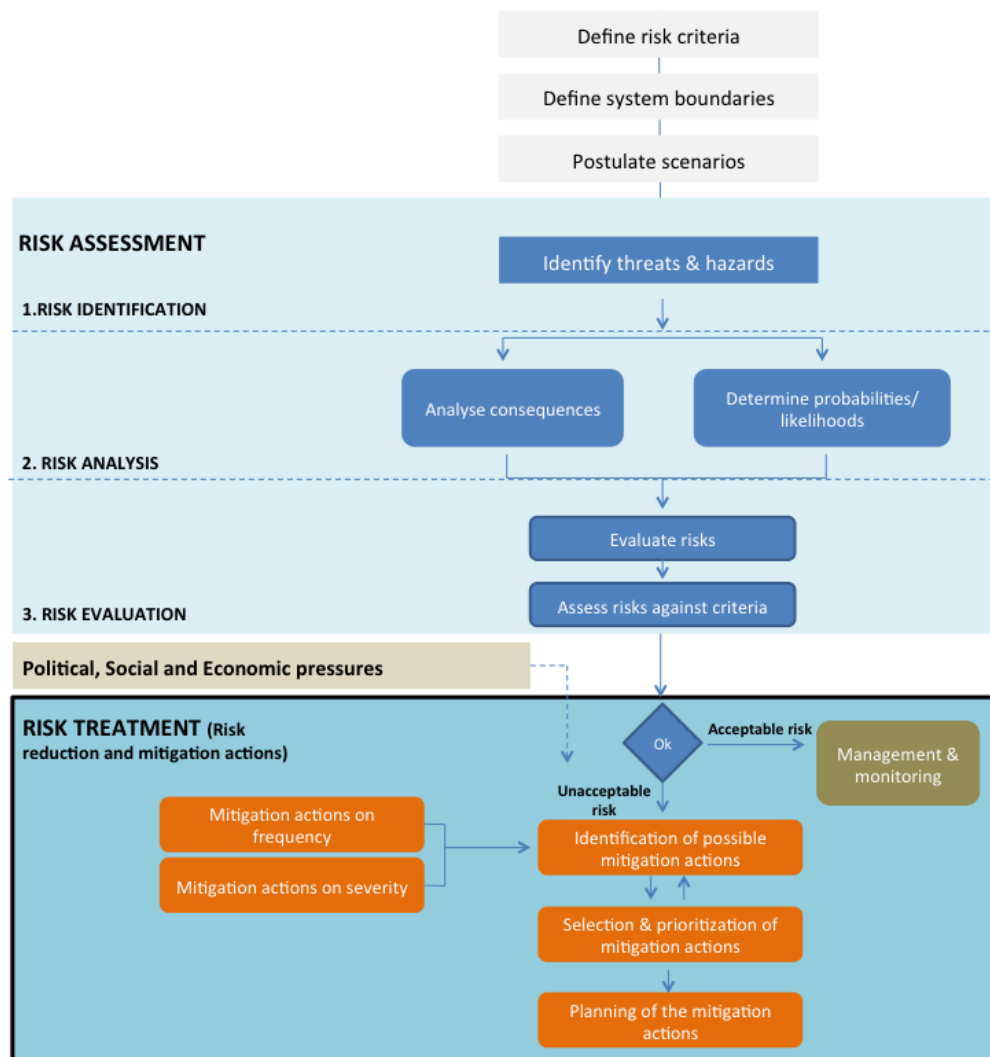


Figure 1: Risk management process with a focus on risk treatment

The first step of the process concerns the evaluation and the comprehension of the context in which the risk assessment is applied (for further details, see D3.2 [1]). It consists in:

- defining the risk criteria (i.e. the terms of reference against which the significance of a risk is evaluated);
- defining system boundaries (i.e. defining the physical and operational boundaries under the

assessment of the mass-gathering event);

- postulating scenarios (i.e. scenarios associated to possible threatening attacks to the crowd, taking into account LEAs' past experiences, private and public sources).

Core phases of the risk management process are the risk assessment and the risk treatment.

The **risk assessment** consists of the following stages: **risk identification** (i.e. Identify threats & hazards), **risk analysis** (i.e. Analyse consequences and Determine probabilities/ likelihoods), and **risk evaluation** (i.e. Evaluate risks and Assess risks against criteria) (see Figure 1). It has been extensively described in D3.2. The risk treatment is the main focus of the D3.3. Within the *risk identification and analysis* it is important to reach a deep understanding of how and why the risk could develop, from its origins down to its possible consequences. It should bring to a deep understanding of the risk in the particular context of the event that is being analysed. It includes the **understanding of the risks root and common causes**, the **evaluation of risk interactions**, and the **identification of all the different aspects of the risks where a mitigation action can be put in place**. The identification of root causes allows understanding the reasons originating the risk and identifying the best preventing action that can operate on the initial conditions at the basis of the risk, making these actions more effective. The identification of common causes between different risks can also lead to more effective mitigation actions, because by addressing the common cause, the action can be able to mitigate all the related risks. Analysis of possible risks interaction involves studying if risks are somehow interlinked with each other, mainly if one risk can cause another one. For example, the risk of a suicide attack could involve an additional risk due to a large crowd trying to evacuate a secluded area. The recent Manchester Arena Bombing³ - where twenty-three people were killed, including the attacker, and over 500 were injured – is an example of this. Some of those injuries were not directly due to the attack but rather to the chaotic evacuation from the Arena. In case a risk may imply a secondary one, the severity need to be adjusted accordingly and the mitigation actions should take both risks into account. In the *risk evaluation* process, results of risk analysis are compared with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable.

Risk treatment deals with events exceeding the risk criteria, identifying measures for risk mitigation. Risks considered not acceptable have an unacceptable combination of frequency and severity. When considering unacceptable risks, it is important to consider also political, social, economic reasons and factors (e.g. for example, the authority may want to avoid any possible major risks to reassure the population after some recent terrorist attacks) that could interfere with the treatment phase of the risk.

In the case of unacceptable risks, the process includes other specific stages, i.e.:

- Identification of possible mitigation actions with a focus on frequency and severity;
- Selection and prioritization of mitigation actions;
- Planning of the mitigation actions.

Each stage will be described in the following sections.

2.2 RISK TREATMENT: MITIGATION MEASURES

On the basis of the risk analysis carried out in the risk assessment, the analyst can decide how to manage the risk. The standard ISO31000 [2] provides principles and guidelines for the management of risk. It

³ <http://www.bbc.com/news/uk-england-manchester-43548173>

suggests the following seven different options for the treatment of risks that are not tolerable:

1. avoiding the risk by deciding not to start the activity (in our case the event) for which the risk assessment has been carried out;
2. accepting the risk, if this is justified by the possible advantages resulting from the activity (opportunities);
3. removing the risk by addressing its root cause;
4. reducing the probability of the risk through adequate prevention actions;
5. reducing the severity of the consequences by means of adequate mitigation actions;
6. sharing the risk with somebody else, for example by subcontracting part of the work implying the risk, or with an insurance covering some of all the costs associated with the risk;
7. accepting the risk with an informed, competent decision.

2.2.1 Identification of possible mitigation actions

The ISO31000 standard [2] applies to risks that can have consequences in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes. That represents any type of risks that an organization can encounter in its activity. The management options listed above shall be evaluated considering the specific type of risk involved and its consequences. Some of the management options are acceptable only for some type of risks, for example a risk can be accepted with an informed decision, when the consequences (and opportunities) are economic but not when there are consequences in terms of safety and security. In particular, the acceptable options in case of event organizations - that will be discussed in the following sections - are those of points 1, 3, 4 and 5.

2.2.2 Avoidance

To cancel the event represents the extreme solution to be applied when no practical mitigation alternatives are available or when all possible mitigations have unacceptable adverse effects. It is also applied when there is no time available for other solutions, for example when a new risk arises or when the probability rises significantly shortly before the beginning of the event. It is a solution that was used in recent cases like the Rock and Ring festival in Nuremburg in Germany where the festival was stopped and people evacuated over 'terror threat', as police issued an urgent security warning. There are several possible adverse effects that need to be evaluated carefully, ranging from obvious economic losses to the feeling of abnormality and anxiety that can be induced in the population to the creation of panic when there is the need for an evacuation [3].

2.2.3 Removing the risk or reducing its probability

The options 3 and 4 of the list of options suggested in ISO31000 [2] and reported above are discussed together here. These options try to prevent the risk effect, reducing its probability, if possible down to zero achieving a full risk removal. For example, the physical creation of vehicle exclusion zones can reduce the probability of conducting a vehicle ramming attack because the attack is difficult to realise. The identification of mitigation actions involves studying how and why the risk could develop, from its origins down to its possible consequences, and personalising the study to the particular context of the event that is being analysed. On the basis of this study different mitigation options can be evaluated, compared, and selected. In the frequent cases in which a full risk removal is not possible, or it is very hard to be obtained at a reasonable cost, the aim becomes to reduce the risk probability to an acceptable level. A possible

secondary effect of the mitigation actions is the deterrence effect on terrorists. In the example discussed above, the physical creation of vehicle exclusion zones could have also a deterrence effect because the terrorist will have more difficulties to fulfil the attack.

Estimating the reduction achieved with mitigation actions can be very difficult. The probability of an attack is usually unknown. Although it is possible to estimate how often many natural disasters will occur, it is very difficult to quantify the likelihood of a terrorist attack, even more the reduction achieved with mitigation measures. In addition, quite often mitigation actions have also a deterrence effect, and the deterrence effect of a certain measure could be even more difficult to be estimated. Deterrence, in the case of terrorism, may also have a secondary impact: after a potential target is hardened, a terrorist may turn to a less protected facility, changing the likelihood of an attack for both targets. Quantitative methods to estimate these probabilities are not available at the moment. To support the choice between different mitigation measures, the assessment team may use a qualitative approach, using expert judgement to make comparisons.

2.2.4 Reduce the severity of the consequences

This option takes place in case an attack cannot be prevented completely, trying to reduce the severity of its consequences. For example, the presence of speed limiting devices can reduce the possibility to accelerate a vehicle in a ramming attack, reducing the consequences of the attack. Reducing the severity consists in studying all the possible consequences of an attack, personalising the study to the particular context of the event that is being analysed, and choosing the best mitigation actions.

As for the probability reduction, estimating the severity reduction can be very difficult. The consequences of an event are linked to the way the event takes place. The usual practice is to consider the consequences of a worst-case scenario and choose among different measures on the basis of the mitigations that could be applied. An expert judgement for comparisons could be useful for this purpose.

2.2.5 Types of mitigation actions

In Section 2.2.4, mitigation actions have been discussed considering their consequences, in particular, if actions have an effect on the probability of a risk (prevention) or on the severity of its consequences (mitigation), or on both. Mitigation actions can also be classified on the basis of the way they are realized. In particular, mitigation actions can be based on:

1. crime prevention through environmental design solutions (i.e. the environmental design to prevent crime);
2. organizational actions;
3. actions based on personnel and related training.

Crime Prevention through environmental design (CPTED)⁴ is based on concrete solutions making the environment more resistant to hazards, or creating physical constraints that are hard to overcome. These are sometimes referred to as **hard mitigation solutions**. An example of engineering or hard mitigation solution is the use of bollards to delimitate the space of an event and create vehicle exclusion zones that can reduce the probability of a vehicle ramming attack (see section 3.2).

⁴ <http://www.popcenter.org/tools/cpted/PDFs/NCPC.pdf>

Organizational solutions are based on improving the organization of the event, revising the assignment of responsibilities and distributing the control on different stakeholders. These are sometimes referred to as **soft mitigation solutions**. An example of organizational or soft mitigation solution consists in making the procurement of vehicles to be used for ramming attacks more difficult by relying on rental companies (see section 3.2). These companies should negate rental of large capacity vehicles if there are suspicions or when renters appear to be “practicing” their large vehicle skills in the time leading up to a nearby open event.

Actions based on personnel rely on preventing risks or mitigating them by training stakeholders involved in the event or related to it. Instructions and training can concern how to communicate with the crowd, how to scrutinize people at the entrance and so on. These are also referred to as **soft mitigation solutions**. An example of action based on personnel consists in making the procurement of vehicles, to be used for ramming attacks, more difficult by sensitizing and training truck drivers. They should reinforce vehicle security during any period during operation or destinations near critical areas (e.g. near parades, sporting events, entertainment venues, shopping centres, or other activities with crowds near roads, streets or venues accessible by vehicles).

2.3 SELECTION AND PRIORITIZATION OF MITIGATION ACTIONS

It is typically not possible to eliminate all the risks associated with events and each event organization has limited resources. This implies that mitigation options must be carefully analysed, selected and prioritized. Selection aims at identifying the following aspects:

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

The selection implies a cost benefit analysis regarding, from one side the effectiveness in terms of reducing the probability of the risk and the severity of its consequences; on the other side, the cost, the acceptability and possible negative impacts of the different mitigation actions. The main elements to be considered are shown in Figure 2.

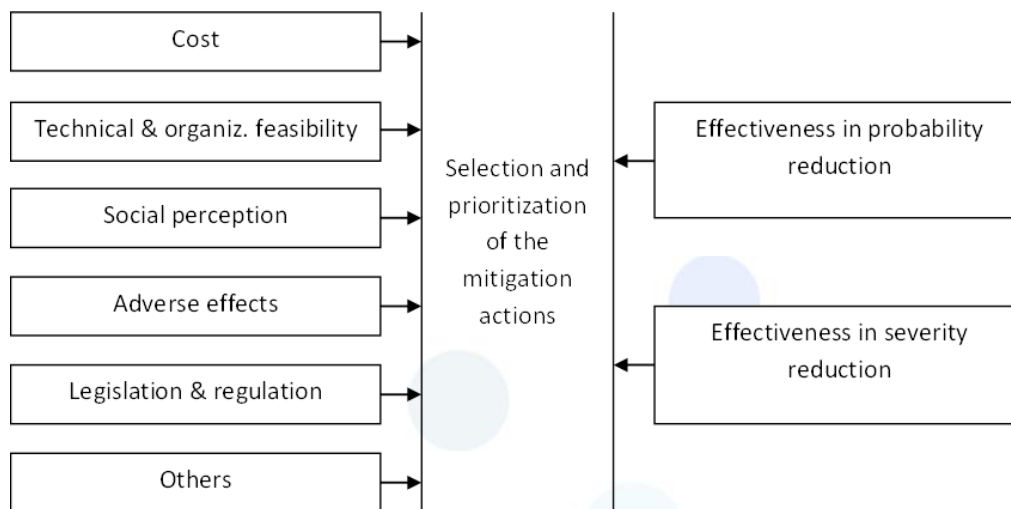


Figure 2: Elements affecting mitigation selection

Effectiveness – It was already discussed why estimating the effectiveness of a mitigation action in reducing the risk probability or its severity is extremely difficult. The most used way is to rely on comparisons based on expert judgment, best practices and past experiences. Comparison should be made considering the possible application of the mitigations in the specific case of the event under consideration.

Cost - To select the mitigation actions it is essential to have an adequate knowledge of the available resources for implementing mitigation options. The amount of financial resources may define the type of mitigation options to be adopted. Each mitigation action has an implementation cost that may limit its applicability. Sometimes the cost can be distributed between the different stakeholders and this may imply a negotiation unless specific responsibilities are stated by law or applicable legislation. In evaluating the cost one should also consider that some actions can bring benefits to several events and, in principle, the costs could be shared between those events. An example is sensitizing and training truck drivers in reinforcing vehicle security in the vicinity of public events. This mitigation action will help in preventing the theft of vehicles to be used for ramming attacks. We can assume that this action will benefit several public events. In some cases there could be national programs available for financing this type of large-scale mitigation measures.

Technical and organizational feasibility - The technical and organizational feasibility represents a clear constraint for the implementation of mitigation actions. Some actions may need highly skilled and specialised engineering expertise for their implementation. Moreover, the implementation may require the coordination of several different stakeholders. Timing can be another limiting factor. Some mitigation actions may need too much time to be realized, and be outside the applicable event deadlines.

Social perception – Social perception of security is a very important element when selecting and identifying mitigation actions. For example, recent damages and disasters can influence the public opinion and require the identification and application of additional and, in some cases, more visible mitigation actions. There is a clear political and social opinion that, after recent terrorist attacks, emphasised that our social life should not change and not be influenced by those events. Since some actions are more visible than others, there is a need to balance between giving a feeling of security to the crowd and avoiding the idea that the event is organized in a “bunker”. Some mitigation actions are based on the contribution of the crowd or of the

community living in the area where the event is organized. In those cases the acceptance of the measures will depend on the understanding of the risks, the reasons for, and the expected benefits of the proposed measures.

Adverse effects – Most of the mitigation actions have adverse effects that shall be carefully evaluated during the selection and prioritization. For example, the deployment of barriers could constraint the movement of the crowd especially during a possible evacuation, or can create obstacles for the intervention of first responders (e.g. ambulances). Some of those adverse effects can be limited through an accurate design and implementation of the mitigation, for example, ensuring the presence of emergency corridors, while others cannot be avoided. Other adverse effect can impact the local population and environment. Some segments of the population may be adversely affected. For example, the construction of barriers and bollards can inhibit the circulation and might influence the local community with effects on and pedestrian mobility. It is also important to consider whether the mitigation options will have a negative effect on environmental assets (e.g. protected natural resources), or other negative effect (e.g. aesthetics of the location).

Legislation and regulation - Different mitigation actions require different authority levels for their implementation. The team in charge of selecting the mitigation actions must identify public authorities and responsible agencies for implementing them and examine their rules and regulations. The team has to identify all legislative problem areas and institutional obstacles as well as the incentives that can facilitate mitigation and implementation. The team will have to balance the mitigation measure against the community's rules and regulations in order to decide which mitigation takes precedence. For example the creation of the security corridor may impact on the transport legislations applied in the area. Without the appropriate legal authority, a mitigation action cannot lawfully be undertaken.

2.4 PLANNING OF THE MITIGATION ACTIONS

Planning the mitigation actions require the identification of resources the schedule and the stakeholders involved with the related responsibilities. The resources shall include budget, people, and equipment that are adequate to implement the mitigation actions. The schedule will have to be realistic and compatible with the deadlines of the event. Some actions may have an impact on local communities for example limiting mobility, in such cases there could be a tight window opportunity for implementing the actions.

3 MAIN RISKS IDENTIFIED IN LETSCROWD AND POSSIBLE MITIGATION ACTIONS

As reported in D3.2 [1] the assessment of risks for mass gathering events typically develops along 3 different phases (see Figure 3):

- Event Preparation;
- Event Execution;
- Post Event.

Mitigation actions presented in the following sections refer to the event preparation phase, including the event planning and the pre-event, thus concerning both the Static Risk Assessment (SRA) and the Dynamic Risk Assessment (DRA) stages for what concerns the event preparation phase.

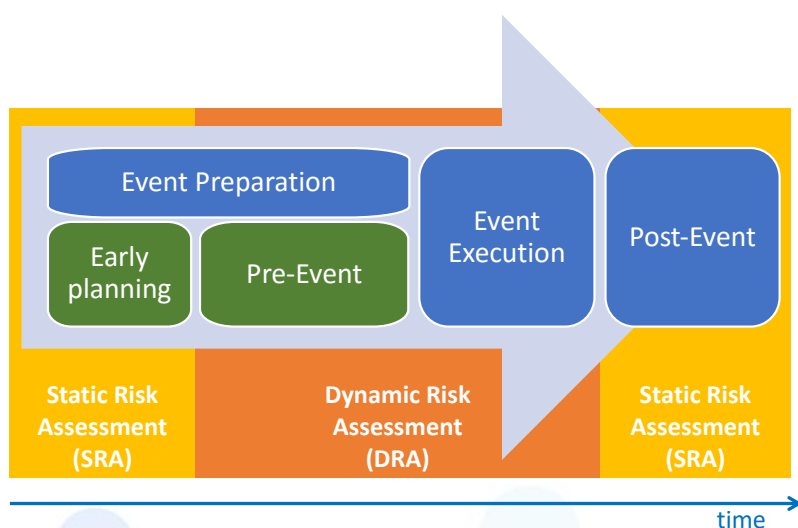


Figure 3: The Static & Dynamic Risk Assessment stages (from D3.2)

D3.2 [1] identified both hazards and threats to be considered when dealing with mass gathering event. The table below summarizes the hazards presented by the crowd and the venue.

Table 1: List of hazards presented by the crowd and by the venue (from D3.2)

HAZARDS PRESENTED BY THE CROWD	HAZARDS PRESENTED BY THE VENUE
Crushing between people	Slipping or tripping due to inadequately lit areas or poorly maintained floors
Crushing against fixed structures, such as barriers	Moving vehicles sharing the same route as pedestrians
Trampling underfoot	People getting trapped, e.g. wheelchair users in a crowd
Surging, swaying or rushing	Collapse of a structure, such as a fence or barrier, which falls onto the crowd
Aggressive behaviour, particularly between groups of rival supporters	People being pushed against objects, such as unguarded, hot cooking equipment on a food stall
Dangerous behaviour, such as climbing on equipment, running down steep slopes or throwing objects	Objects, such as stalls, that obstruct movement and cause congestion during busy periods
Spontaneous panic (e.g. misunderstanding of the situation, ...)	Crowd movements obstructed by people queuing
	Cross flows as people cut through the crowd to get to other areas, such as toilets
	Failure of equipment, such as turnstiles

Sources of fire, such as cooking equipment

As already specified in D3.2 [1], the hazards above are not at the core of LETSCROWD. However, they have to be considered since they may intervene after a security threat manifests, influencing the severity of the consequences for the crowd (possible cascade effects). These types of hazards will be addressed in the second version of this deliverable (D3.7). D3.3 aims at exploring and describing only the **security threats** related to mass gathering events and identified in D3.2 [1]. More specifically, the risks considered are those related to terrorism (see Table 2). Mitigations have been identified with regards to the attack modes by which security threats can occur.

Table 2: List of risks related to terrorism and the proposed mitigations

Threat	Attack mode	Mitigations	Type of mitigation
Terrorism	Vehicle used as weapon (vehicle ramming)	Barriers and creation of vehicle exclusion zones	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	Hard (CPTED 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	Hard (CPTED solution)
		Training for detection of possible attacks	Soft (action-based on personnel)
	Cold steel (e.g. stabbing)	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	Creating awareness on the use of trusted SN channels	Hard (CPTED solution)
		Identifying trusted channels for cultural minorities	Soft (action-based on personnel)
		Counteract the spread of misinformation	Soft (organisational solution)
		Mitigating the Crowd-turfing by the use of automated crawling systems that are able to identify fake messages	Soft (action-based on personnel)
	Mitigating the Crowd-turfing by the use of automated crawling systems that are able to identify fake messages		Hard (CPTED solution)
	Shooting	Body search	Soft (organisational solution)
		Walkthrough metal detector (WTMD)	Hard (CPTED solution)

	X-ray scanning machine Training for identification of suspicious signs in behaviour and appearance	Hard (CPTED solution) Soft (action-based on personnel)
Combined attack (two or more attacks simultaneously launched against the event)	Combination of several mitigations	

For each risk, the description of the mitigation actions currently applied has been provided.

3.1 MITIGATION ACTIONS: STRUCTURE AND COMPONENTS

In the following sections the mitigation actions are presented including:

- a short description of the risk;
- a description of the reasonable worst-case scenario based on literature;
- a description of the possible existing mitigation actions by detailing:
 - the possible effects on frequency and severity;
 - the potential adverse effects;
 - the stakeholders responsible for implementing the mitigation action.
- a description of possible mitigations resulting from research and the work carried out in the LETSCROWD project.

Generally speaking, mitigations are not universal and shall be selected on the basis of the characteristics of the event under analysis 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.

That's why only generic information is provided for each mitigation, together with an extensive bibliography. Using the references the reader will be able to customize the mitigation actions to the specificity of the event under consideration.

3.2 VEHICLE-RAMMING ATTACK

3.2.1 Description of the risk

A **vehicle-ramming attack** is a form of attack in which a perpetrator deliberately rams a motor vehicle into a crowd of people. Vehicle ramming offers terrorists with limited access to explosives or weapons an opportunity to conduct an attack with minimal prior training or experience. The earliest known use of a vehicle-ramming attack took place in 1973 by a woman with psychiatric problems (Olga Hepnarová) who drove her truck into a group of about 25 people waiting for a tram in Prague, killing 8 people. Starting from the beginning of the century this type of attack has been widely used by terrorists [4]. Online terrorist media continues to inspire and incite individuals to use a vehicle as a weapon as an attack. A complete list and timeline of these events is available at [4]. Future internet-connected self-driving cars can represent a new instrument for this type of attack. These cars can potentially be hacked remotely and used for ramming attacks. Such an additional risk will have to be carefully evaluated and mitigated in the future.

3.2.2 Reasonable worst-case scenario

It is difficult to define a worst-case scenario because severity is linked to the characteristics of the environment where the attack takes place. Elements that influence the consequences and eventually make the case worst are: type of vehicle and related mass; type of ground (e.g. concrete, mud, asphalt) where the attack is perpetrated with the associated possibility to gain and maintain speed; size of the event and concentration of the crowd; presence of other vehicles or obstacles that can hamper the attacking vehicle. As an example of worst-case scenario one could consider an attack with an heavy truck, with a long stretch of paved road to gain speed and with high density crowd distributed along the road (like in a march or protest) where speed can be easily preserved. This is similar to what happened in 4 July 2016, where a 19 tonne cargo truck was deliberately driven into crowds of people celebrating Bastille Day on the Promenade des Anglais in Nice, France, resulting in the deaths of 86 people and the injury of 458 others [5].

3.2.3 Possible existing mitigation actions

A vehicle ramming is a very efficient form of attack very hard to mitigate. The Berlin's police chief, Klaus Kandt, after the attack on Christmas market in Berlin evidenced how the number of potential targets is so large that is extremely difficult to prevent attacks, "*... the measures to achieve to mitigate the risk are varied, complex, and do not represent an universal panacea*"⁵. In the following we give an overview of the most common possible mitigation actions whose applicability and effectiveness need to be evaluated case by case.

3.2.3.1 Barriers and creation of vehicle exclusion zones

3.2.3.1.1 Description

This is 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. The US state department "anti-ram vehicle list" lists several types of bollards and other physical barriers such as spike strips to protect the perimeter of embassies and other sensitivity targets abroad [6]. Some bollards are capable of stopping vehicles travelling at up to 80 km/h. Several references are available to design and implement barriers and speed limiting solutions, see for example [7] and related guidance material, or [8]. National and International Standards regulate their production, testing and installation [9], [10], [11], [12].

3.2.3.1.2 Possible effects on frequency and severity

Barriers, solutions to reduce speed and creation of vehicle exclusion zones can mitigate both the probability and severity of vehicle ramming attacks. In particular, the adoption of these solutions can dissuade terrorists in advance because of the difficulties they would encounter in realizing the attack, impede the perpetration of the attack once it has been tried, and reduce the consequences if the attack is successfully perpetrated. Well-organized barriers have proven their positive influence on both frequency and severity in real cases. For example, in the 2014 Alon Shvut stabbing attack, barriers prevented ramming, leading the

⁵ <https://www.theguardian.com/uk-news/2016/dec/20/what-can-be-done-to-prevent-berlin-style-attacks-in-modern-cities>

terrorist to abandon his car and attack pedestrians waiting at a bus stop with a knife, after his effort to run them over was frustrated [13]. In the 2007 Glasgow Airport attack Security bollards are credited with reducing the speed of the vehicle entering the terminal, minimizing damage and casualties [14].

3.2.3.1.3 Potential adverse effects

In addition to the significant cost of a wide deployment of barriers the main potential adverse effects are related to the movement of the crowd and the possible feeling of abnormality and anxiety that can be generated by the measures. The influence of the presence of barriers on the movement of the crowd has been investigated in depth by the UK Department for Transport. Reports of the studies and guidance material are available for both normal conditions [15], [16] and emergency [17]. The important thing for public sanity is that people remain able to go about their normal working and leisure times blissfully unaware that there is a risk that has been considered and reduced or eliminated. Designers have got the technology to create aesthetically pleasing barriers to prevent cars from ramming into buildings [18]. For example, flower pots can actually be enforced with concrete and metal to prevent a truck from going over them. They are hidden and blended into the aesthetics of the environment. A full line of study has been dedicated to the design of proportionate and aesthetically pleasant counter terrorism features in new and existing developments planned for crowded public places [3].

3.2.3.1.4 Stakeholders responsible for implementing the mitigation action

Stakeholders responsible for implementing the action depend on the type of installation (e.g. permanent, temporary), the location (e.g. public or secluded area) and local regulations. These stakeholders typically include: local administrations, LEAs, and event organizers.

3.2.3.2 Sensitize and Training for detection of weak signals

3.2.3.2.1 Description

There are several possible indicators that may suggest the preparation of a vehicular terrorist attack. These include for example: modification to the vehicle such as homemade attempts to reinforce the front of the vehicle with metal plates; apparent driver unfamiliarity with a commercial motor vehicle; purchase, rental, or theft of large vehicles accompanied by typical indicators such as nervousness during the purchase, or paying in cash; commercial motor vehicles being operated erratically, at unusual times, or in unusual locations. Examples and descriptions of indicators are available from the US Federal Bureau of Investigation [19] and from the US Transportation Security Administration [20]. As usual, although a single indicator may not be suspicious, one or more might indicate a ramming attack is being prepared or developed. 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.

3.2.3.2.2 Possible effects on frequency and severity

The main contribution of sensitizing and training for detection of weak signals is on frequency of the event. It has a preventive effect, lowering the frequency of the attacks. There are no data to estimate the real contribution of a widespread collaboration by all the stakeholders, but an overall consensus among experts worldwide about the importance of this mitigation action as a complement to other actions [19], [20], [21].

3.2.3.2.3 Potential adverse effects

There are two main adverse effects influencing the feasibility of this mitigation. The first one is the number of false alarms that could result from a widespread collaboration of all the stakeholders involved. It can be extremely expansive, in terms of effort and time, to verify all the reports. On the other hand the consequences of ignoring a report can lead to dramatic consequences and responsibilities. In addition, the collaboration of the stakeholders will continue only if reports are seriously considered. It is very difficult to find an adequate balance in the filtering of the reports. The experience in other domains [22] has shown that an important contribution can come from a precise definition and clear instructions to the stakeholders about when and what to report.

3.2.3.2.4 Stakeholders responsible for implementing the mitigation action

Stakeholders responsible for implementing the action are mainly LEAs that should promote and sensitize stakeholders about reporting. The commercial vehicle industry and the car rental companies are responsible for involving and training their staff.

3.2.3.3 Control on vehicle rental and operation

3.2.3.3.1 Description

A possible mitigation action regarding this risk 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 [4]. Mitigation should focus on this specific phase of the attack preparation. Mitigation actions of this type include for example: reinforce vehicle security during any period, or during operation or destinations that are near parades, sporting events, entertainment venues, shopping centres, or other activities with crowds near roads, streets or venues accessible by vehicles; instruct drivers to keep vehicles locked while in operation and while parked, instruct drivers to be suspicious of any unknown person who approaches them or attempts to enter the vehicle while in route; negate rental of large capacity vehicles if the rental raise doubts and rental is near critical areas or when renters appear to be “practicing” their large vehicle skills in the time leading up to a nearby open event. Examples of these mitigation actions are available [20].

3.2.3.3.2 Possible effects on frequency and severity

The main contribution of actions hindering the procurement of the vehicle is on frequency of the event. It has a preventive effect, lowering the frequency of the attacks. There are no data to estimate the real contribution of a widespread collaboration by all the stakeholders, but an overall consensus among experts worldwide about the importance of this mitigation action as a complement to other actions [19], [20], [21].

3.2.3.3.3 Potential adverse effects

The main adverse effect influencing this mitigation is linked to the reaction of the terrorists when a driver or the vehicle rental staff resists to their actions (e.g. negate the rental, react to their effort to enter the vehicle).

3.2.3.3.4 Stakeholders responsible for implementing the mitigation action

Stakeholders responsible for implementing the action are mainly LEAs that should sensitize truck drivers and car rental staff to adopt this careful behaviour. The commercial vehicle industry and the car rental companies are responsible for reinforcing this message to their staff.

3.3 IMPROVISED EXPLOSIVE DEVICES (IEDS)

3.3.1 Description of the risk

The term IED came into common usage during the Iraq War that began in 2003⁶. An improvised explosive device is most commonly defined as “a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from non -military components” [23].

Explosives and bombs remain one of the most favoured terrorist weapons used by criminal organizations, terrorist groups and extremist individuals for their ability to inflict mass casualties, cause fear and disruption, and attract media attention [24]. It is not difficult to understand why IEDs have increased in popularity as the weapon of choice by terrorists. “They are cheap, easy to make and hide, and their employment tactics techniques and procedures are very flexible and difficult to counter” [25].

Because they are improvised, they can be produced in varying sizes and delivered in a number of different ways. Terrorists often conceal them within electrical or electronic items. “Items, like laptop computers, hairdryers, disk-drives, radios, cameras, mobile phones, etc., have so many different components packed into a relatively small area that an IED hidden within such items can be extremely difficult for an X-ray screener to detect”⁷.

IEDs can be remotely used. They can employ a number of different methods to initiate the explosion [24]. Concerning this, the function categories of IED most commonly used are:

- time fired (i.e. IED detonates after pre-set time delay);
- victim activated (i.e. IED detonates by actions of unsuspecting individuals);
- command operated (i.e. Bomber chooses optimum moment to detonate IED, for instance by means of cell phones, radios/ transmitters/ receivers, car alarms, command wire etc.)⁸.

Landmarks, special events, critical infrastructure, transportation systems, places of worship, and especially commercial premises and markets are common targets for these types of explosives. Between 2011 and 2016, Action on Armed Violence (AOAV) has recorded 124,317 deaths and injuries from IEDs, of which 81% (100,696) were civilians. The first half of 2017 has seen a further 7,784 deaths and injuries. In 2017 the worst impacted countries from IEDs were Iraq, Afghanistan, Syria, Pakistan and Somalia, among them Afghanistan has consistently been amongst the countries worst impacted by IEDs year on year [26].

IEDs typically fall into three types of categories: 1) Package Type IED; 2) Vehicle-Borne IEDs (VBIEDs); 3) Suicide Bomb IED⁹. Types 2 and 3 add specific characteristics to the main general category described above and directly concerning the type 1.

⁶ https://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf

⁷ <http://www.x-rayscreener.co.uk/?xray=improvised-explosive-devices>










⁸ <https://www.slideshare.net/OFFSHC/offshc-gets-briefed-on-ieds>

⁹ <https://www.globalsecurity.org/military/intro/ied.htm>

Vehicle-Borne IEDs

Vehicle borne IEDs (VBIEDs) are devices that use a vehicle as the package or container of the device¹⁰. They differ in size and in components (e.g. gas cylinders, petrol, nails, etc.), also according to the type of vehicles chosen (from sedans to cargo trucks). Larger vehicles enable the employment of larger amounts of explosive. These are vehicles driven to and detonated near a given target, thus they have a huge potential to cause large numbers of casualties and significant damage to buildings and infrastructures. The VBIED can either be parked or then remotely detonated, or a suicide bomber - who ultimately controls the detonation mechanism - can drive it. The latter is defined as a *Suicide Vehicle Borne Improvised Explosive Device* (SVBIED), or more commonly: *a suicide car bomb* [26].

As shown in Figure 4, a maximum explosive capacity, a lethal air blast range and a minimum evacuation distance can be estimated with regards to different vehicle categories (data provided by the U. S. Department of Homeland Security¹¹). The stand-off distance is the most important factor in determining the extent of damage for a given-size VBIEDs [27].

 BOMB THREAT STAND-OFF CHART			
Threat Description Improvised Explosive Device (IED)	Explosives Capacity ¹ (TNT Equivalent)	Building Evacuation Distance ²	Outdoor Evacuation Distance ³
 Pipe Bomb	5 LBS	70 FT	1200 FT
 Suicide Bomber	20 LBS	110 FT	1700 FT
 Briefcase/Suitcase	50 LBS	150 FT	1850 FT
 Car	500 LBS	320 FT	1500 FT
 SUV/Van	1,000 LBS	400 FT	2400 FT
 Small Moving Van/ Delivery Truck	4,000 LBS	640 FT	3800 FT
 Moving Van/ Water Truck	10,000 LBS	860 FT	5100 FT
 Semi-Trailer	60,000 LBS	1570 FT	9300 FT

1. These capacities are based on the maximum weight of explosive material that could reasonably fit in a container of similar size.
2. Personnel in buildings are provided a high degree of protection from death or serious injury; however, glass breakage and building debris may still cause some injuries. Unstrengthened buildings can be expected to sustain damage that approximates five percent of their replacement cost.
3. If personnel cannot enter a building to seek shelter they must evacuate to the minimum distance recommended by Outdoor Evacuation Distance. These distance is governed by the greater hazard of fragmentation distance, glass breakage or threshold for ear drum rupture.

Figure 4 - Explosive evacuation distance according to the different IEDs types

¹⁰ <https://www.globalsecurity.org/military/intro/ied.htm>

¹¹ <https://publicintelligence.net/dhs-bomb-threat-stand-off-chart/>

Suicide Bomb IED

A suicide bomber is defined in the Cambridge Dictionary as: “a person who has a bomb hidden on his or her body and who kills himself or herself in the attempt to kill others” [28]. The concealment of weapons and low cost to make a bomb means the effects of a suicide bombing can be deadly [29]. The bomber also needs no escape plan, which is often one of the most difficult and complex parts of planning a terror attack [29].

[30] describes important tactical advantages of suicide bombings such as: higher lethality, psychological and social impact, wide media coverage, communication of relevant messages to target audiences (determination, commitment to escalate, deterrence of neutral observers, shaming the enemy, solicitation of recruits).

Moreover, most suicide attacks are not isolated incidents but are grouped in [31]. The instigators that promote such actions choose the method among others in order to achieve certain strategic goals [31]. Brussels Airport attack on 22nd March 2016 has been linked to the November 2015 Paris Attacks for example. However, after the event Police indicated that the 22nd May 2017 Manchester Arena attacker acted alone, although this was potentially religiously motivated.

Suicide attacks, as with other types of terrorism can be seen as a means to an end; a tactic that anyone could use, and is unlikely to be a consequence of “root causes” such as political oppression [32].

The potential risk to mass gatherings of a suicide bombing is evident as this has happened in the noted examples and other events with seemingly different reasons behind the attacks.

3.3.2 Reasonable worst-case scenario

It is difficult to define the worst-case scenario related to this types of threat because the severity might vary according to: 1) the features of the physical layout of the environment; 2) the number of people attending an event; 3) IEDs types and related amounts of explosive used to carry out the attack; and 3) combination of several IEDs types in the same attack, creating a hybrid complex scenario (i.e. package; VBIEDs/ SVBIED).

Incidents involving IEDs include:

- **IED** - Boston Marathon bombings: the Boston Marathon Bombing was a terrorist attack that occurred on April 15, 2013, when two bombs went off near the finish line of the Boston Marathon, killing three spectators and wounding more than 260 other people¹²;
- **VBIEDs** - Madrid car bombs injured 16 people outside Real Madrid's football stadium before the European Champions League semi-final, on 1/05/2002. Two car bombs, packed with 20 kilos of explosives, were parked 150 yards away from the Santiago Bernabeu stadium. Basque separatist group ETA claimed responsibility for the bombs¹³;
- **VBIEDs** - London car bombs (discovered and disabled before they could be detonated) on 29/6/2007. One of the two cars was discovered by an ambulance crew called to a nightclub to treat a person. They noticed a Mercedes parked outside the club having smoke inside it. Witnesses

¹² <https://www.history.com/topics/boston-marathon-bombings>

¹³ <https://www.theguardian.com/world/2002/may/02/football.spain>

saw the car being driven erratically earlier, and crashing into bins before the driver ran away. Car contained gas cylinders, petrol and nails. They were similar to car bombs used in Iraq¹⁴;

- **Suicide bomber** - Manchester bombing attack: a suicide bomber killed 22 people and injured more than 500 by remotely detonating a home-made bomb (packed in a £20 *Karrimor* backpack) in the Manchester Arena at the end of an Ariana Grande concert¹⁵ [33];
- **Suicide bomber** - November 2015 Paris attacks: coordinated multiple suicide bombers (or shooting attacks where the attackers then killed themselves) across multiple locations killed [34].

Concerning the **VBIEDs**, different techniques have been applied in war zones to enhance the bomb blast effect. One of them consists in involving multiple vehicles in the attack. A vehicle works as the lead one, used as a decoy or barrier buster. Once stopped, with security forces detaining it and/ or starting the inspection, the main VBIED comes crashing through and into the crowd before detonating. Thus resulting in high increase of casualties¹⁶. Factors contributing to depict the worst possible scenario could be: the vehicle capacity associated with the amount of explosive that can be employed; types of explosive materials used and their combination; security measures in place; coordination among more IEDs attacks during a short time (including package type IED, VBIEDs/ SVBIEDs); and VBIED location. According to this last point, the critical location of a VBIED is a function of the site, its physical characteristics and the venue layout. As explained by FEMA (U.S. Federal Emergency Management Agency): “For vehicle bombs, the critical locations are considered to be at the closest point that a vehicle can approach on each side, assuming that all security measures are in place. Typically, this is a vehicle parked along the curb directly opposite the building [e.g. *where the event takes place; editor’s note*], or at the entry control point where inspection takes place” [27] . If a VBIED is driven to or parked in a high crowded place, its destroy impact is huge. This is the case of one of the worst VBIED attack occurred in Baghdad, on 3th July 2016, during Ramadan, with 341+ deaths and injured hundreds more. ISIS militants carried out a coordinated bomb attacks, involving four IEDs bombings during the day. One of the IED was concealed inside a refrigerator truck driven by a suicide bomber in the heart of the city (the district of Karrada), filled of stores and popular restaurants. Terrorists used a new tactic, which helped them to move undetected through checkpoints. The Iraqi Civil Defence Force confirmed that the mix of chemicals for the bomb was unique, never used before in Iraq. The fire caused by the bombing trapped people in shopping centres, which lacked any emergency exits¹⁷.

There are many examples of **suicide bombings** in crowded places in recent years, with one in Iraq noted as the worst ever on 3rd July 2017, with 250+ deaths. This was a vehicular suicide bombing at the end of Ramadan [35]. Section 3.3.6 will deal with non-vehicular suicide bombings where one or more people have explosives strapped to their person. The recent major example in terms of death and injury in Europe are currently the November 2015 Paris attacks, which were coordinated with multiple suicide bombers (or shooting attacks where the attackers then killed themselves) across multiple locations [34].

The Manchester Arena bombing was a single suicide bomber, who killed 22 people and injured at least 512 people [33]. This type of threat requires fewer organisations than the more complicated attacks and would

¹⁴ <https://www.theguardian.com/uk/2007/jun/29/terrorism.uksecurity>

¹⁵ <https://blogs.state.gov/stories/2017/07/17/en/us-policies-and-actions-aim-counter-improvised-explosive-device-threats>

¹⁶ <https://www.globalsecurity.org/military/intro/ied.htm>

¹⁷ https://en.wikipedia.org/wiki/2016_Karrada_bombing

therefore likely occur at a higher frequency in terms of risk. A worst-case could be considered multiple attacks on one mass gathering similar to these attacks.

3.3.3 Possible existing mitigations common to the three types of IED attacks

IEDs attacks are very difficult to be prevented because can be delivered in different forms and they can be easily concealed. “IEDs cannot be stopped — they can only be mitigated and managed”¹⁸. The following sections present common and specific mitigation actions that can be used to prevent this type of terroristic attack.

3.3.3.1 Counter –IEDs awareness and training in suspicious behaviours

3.3.3.1.1 Description

To reduce risk of IED threats, training courses to build counter-IED capabilities, enhance awareness of IED threats, be alert for suspicious behaviour and IED indicators is the most common and effective defence. 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). Training curricula comprise, for instance, the *Bombing Prevention Awareness* [36], including IED and Homemade Explosive awareness, explosive effects mitigation, protective measures awareness, suspicious behaviours, etc. [36]. Among them, training in suspicious behaviours identification is probably one of the most relevant mitigation measures to be applied. Law enforcement agencies, security staff and other relevant stakeholders, should be able to recognize a nervous behaviour that appears suspicious in certain circumstances, even if it may be typical in other ones. Identifying suspicious behaviours is a matter of context. It needs an informed assessment based on the environment, experience, judgment and common sense.

LETSCROWD project will develop a crowd protection-training package for enhancing the “human factor” capabilities as “security sensor” (D7.6, due at M26). These capabilities also include recognizing suspicious activities, and providing immediate and proper emergency responses to suspicious items and patterns (identified in D3.1).

3.3.3.1.2 Possible effects on frequency and severity

The main contribution of sensitizing and training for Counter-IEDs awareness and detection of suspicious behaviours is on frequency of the event. It has a preventive effect, lowering the frequency of the attacks. There are no data to estimate the real contribution of a widespread collaboration by all the stakeholders, but an overall consensus among experts worldwide about the importance of this mitigation action as a complement to other actions.

3.3.3.1.3 Potential adverse effects

Concerning the suspicious behaviours identification, the main adverse effect may be the attitude to classify people from different cultural backgrounds as suspicious due to the perception of differences that can be misunderstood. People could be worthy of particular attention since they belong to specific minority cultural groups. In other terms, they could be discriminated for the group or category to which they belong or to which someone thinks they belong.

¹⁸ <http://www.securityinfowatch.com/article/10921839/ways-to-mitigate-risk-from-improvised-explosive-devices>

3.3.3.1.4 Stakeholders responsible for implementing the mitigation action

Stakeholders responsible for implementing the action typically include: venue security staff, security screeners, LEAs and event organizers.

3.3.4 Package Type IED: specific mitigation actions

3.3.4.1 Explosive detection system

3.3.4.1.1 Description

Explosive detection systems are widely used in different contexts, sensitive targets and high-risk sites (e.g. airports, train stations, governmental buildings, major events, etc.) to scan bags and luggage of people in controlled access points.

Generally speaking, 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 scenarios¹⁹. Concerning package type IEDs, explosive trace detection may involve swabbing surfaces — such as hands, bags, table tops, etc. — to find miniscule amounts of a variety of explosives (e.g. airport screening system)²⁰.

3.3.4.1.2 Possible effects on frequency and severity

Explosive detection systems are likely to reduce frequency and severity of a package IED attack since they can quickly detect if a bag or a luggage contain a potential threat.

3.3.4.1.3 Potential adverse effects

Explosive detection systems do not make autonomous decisions for acceptable and reliable threat detection. Final assessment and decision heavily depend on human operators who interpret images. Weapons, knives and IEDs can be hardly detected, when they are not viewed from a familiar side profile. For example, if the weapon is viewed from above or from its end, it will be far more difficult to identify²¹. It could represent a potential adverse effect. Because it is difficult to predict how terrorists will conceal/position weapons and IEDs, screeners need to be trained to recognise threat items from all viewpoints.

“Furthermore, the problem of spotting IEDs with explosive detection systems (e.g. x-ray) is further complicated by the fact that plastic explosives have densities and characteristics which make them appear similar to many non-threat, organic materials (such as plastic, leather, rubber, paper, textiles and foodstuffs) routinely contained in carry-on baggage. If explosives are present in a packed bag they will

¹⁹ https://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf

²⁰ <http://www.securityinfowatch.com/article/10921839/ways-to-mitigate-risk-from-improvised-explosive-devices>

²¹ <http://www.x-rayscreener.co.uk/?xray=x-ray-limitations>

almost certainly be partially or completely obscured by denser innocuous objects. The design of IEDs is continually changing and evolving”²².

3.3.4.1.4 Stakeholders responsible for implementing the mitigation action

All the stakeholders involved in the IEDs detection, e.g. security screeners, employees, first responders, military personnel.

3.3.5 Vehicle-Borne IEDs (VBIEDs): specific mitigation actions

3.3.5.1 Vehicle surveillance and control/ inspection

3.3.5.1.1 Description

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.

As described in [24] [37], there are particular indicators unique to VBIEDs that should be considered when assessing suspicious or unattended vehicles, including:

- unusual items inside a vehicle (gas cylinders, petrol cans, electrical wires, leaflets, large bags or boxes, and extra batteries);
- indications of a triggering device (visible wires, switches, radio transmitter, timer, inside or on vehicle);
- presence of the vehicle in an area where it should not be, parked illegally, or near authorized vehicle entrances or crowded access points;
- recent alterations or repairs;
- large containers on seats or cargo area: bags, boxes, barrels, tanks;
- odour of gasoline, propane, acids, or chemicals;
- licence plates inconsistent with vehicle registration;
- rental vehicles with false papers.

3.3.5.1.1 Possible effects on frequency and severity

Vehicle surveillance and control/ inspection can mitigate the probability of VBIEDs attacks, making more difficult the access to target and, thus, the planned realization of the attack.

3.3.5.1.2 Potential adverse effects

Countermeasures have relevant effects in terms of costs (e.g. personnel cost/ resources availability) and impact, for instance, on traffic circulation, making it less smoothly and requiring more effort to be managed. In case of high density of circulation, these countermeasures can affect people’s reactions, generating non-cooperative behaviours that can be difficult to handle by security staff. Vehicle surveillance and control/ inspection can have a potential adverse effect on people’s risk perception about the event, triggering anxiety and facilitating concerned reactions.

In case of a VBIED is driven by a suicide bomber (e.g. along the close public roadways leading to event

²² <http://www.x-rayscreener.co.uk/?xray=x-ray-limitations>

venue), the vehicle control and inspection carried out by the security forces at check-points, could lead the suicide bomber to blow himself to avoid the possibility to be recognized²³.

3.3.5.1.3 Stakeholders responsible for implementing the mitigation action

All the stakeholders involved in the VBIEDs surveillance and controls, e.g. security services, LEAs, military personnel.

3.3.5.2 Anti-ram vehicle barriers

3.3.5.2.1 Description

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 [27]. 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. According to FEMA, stand off distance is measured from the center of gravity of the charge located in the vehicle to the building under analysis, considering the types of VBIEDs and their explosive capacities (see Figure 4).

Determination of minimum distances is specific for each building/ infrastructure and is based on [27]:

- prediction of the explosive weight of the VBIED;
- required level of protection: this may be specified in the case of a government building (e.g. in case of political demonstrations), but for a privately owned building (e.g. hosting an event organized by a private organizer), it is a determination of the “acceptable risk” made during the risk assessment process;
- revaluation of the type of building construction;
- constraints or opportunities provided by the site.

3.3.5.2.2 Possible effects on frequency and severity

Anti-ram barriers - creating vehicle exclusion zones - can mitigate both the probability and severity of VBIEDs attacks. The adoption of this solution can both dissuade terrorists and reduce the consequences if the attack is successfully perpetrated, because it could guarantee the necessary stand-off distance.

3.3.5.2.3 Potential adverse effects

The cost/performance of the perimeter barriers - evaluated in relation to the entire protection system – could be significantly relevant. In addition, others potential adverse effects are related to the possible feeling barriers may generate in the crowd [15], [16].

3.3.5.2.4 Stakeholders responsible for implementing the mitigation action

Stakeholders responsible for implementing the action depend on the type of installation (e.g. permanent, temporary), the location (e.g. public or secluded area) and local regulations. These stakeholders typically include: local administrations, LEAs, and event organizers.

²³ <http://www.bbc.com/news/world-middle-east-27990202>

3.3.6 (Squad of) Suicide bomber (s): specific mitigation actions

Suicide attacks are generally perpetrated without warning [38]. This makes them difficult to mitigate against, hard to predict and identify without prior warning. However, there are existing mitigation measures that have been identified as follows.

3.3.6.1 Physical Barriers

3.3.6.1.1 Description

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 [39]. 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.

3.3.6.1.2 Possible effects on frequency and severity

The perimeter barriers will reduce the frequency of attacks by dissuading potential terrorists, although this may just displace them to a different mass gathering that is easier to access without being seen. The severity of an attack could also be mitigated by forcing the detonation of the bomb away from crowded areas, outside the barrier design.

3.3.6.1.3 Potential adverse effects

It may not be possible to barrier the mass gathering area and limit the number of entry points. For example, street parades, on street sports events such as cycling etc. are generally open to all, with no tickets or restrictions to entry and over wide areas making this mitigation impractical.

This restriction needs to be carefully planned, as emergency exits will be required if an incident were to occur, and barriers should not prevent this.

3.3.6.1.4 Stakeholders responsible for implementing the mitigation action

Stakeholders responsible for implementing the action depend on the type of installation (e.g. permanent, temporary), the location (e.g. public or secluded area) and local regulations. These stakeholders typically include: local administrations, LEAs, and event organizers.

3.3.6.2 Security and Id Checks

3.3.6.2.1 Description

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.

3.3.6.2.2 Possible effects on frequency and severity

This measure is mainly a deterrent, making it more difficult for the suicide bomber to enter the event with a bomb on their person. This lowers the frequency of an attack, and removes the likelihood of a larger bomb being detonated, reducing severity. These amounts are not quantifiable.

3.3.6.2.3 Potential adverse effects

The security checks on entry are generally very slow, meaning long queues to enter the event. These areas in themselves are crowded and could be a potential location for a suicide bombing. The Manchester Arena attacks occurred near exits, which had not been secured throughout the event being live, so entry security checks would not have prevented the attack.

3.3.6.2.4 Stakeholders responsible for implementing the mitigation action

The event organisers and LEAs would be responsible for carrying out such checks.

3.3.6.3 Sniffer Dogs

3.3.6.3.1 Description

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.

3.3.6.3.2 Possible effects on frequency and severity

This measure will be able to detect a suicide bomber in person, but would mainly be a deterrent to the suicide bomber attending as they may be discovered. Therefore, it would reduce the frequency of risk.

3.3.6.3.3 Potential adverse effects

Dogs may not be welcomed by all visitors, making them feel uncomfortable. If a suicide bomber feels threatened by the dog, they may detonate the device immediately.

3.3.6.3.4 Stakeholders responsible for implementing the mitigation action

LEAs are responsible.

3.4 CBRN ATTACK

3.4.1 Description of the risk

The threat of terror organizations using chemical, biological, radiological, and nuclear (CBRN) materials to mount attacks is a serious cause of concern to law enforcement agencies around the world. Intelligence reports indicates that terror organizations, and first and foremost – the World Jihad organizations – are making efforts to obtain the know-how and means required for the production of weapons of mass destruction. Some terror organizations have already obtained the capacity to carry out terror attacks using non-conventional means. Examples include:

- January 14, 2003²⁴ – four terrorists were arrested in London, England, after British police raided two addresses in northern and eastern London, and discovered traces of ricin, one of the world's deadliest poisons;
- February 2002²⁵ – suspected terrorists in Rome, Italy where detained with quantities of cyanide and maps of the U.S. embassy and the city's water supply system;
- 2001²⁶ – US army forces in Afghanistan captured a video showing al Qaeda experiments using chemical substances on dogs;
- The 2001 anthrax attacks in the United States²⁷ occurred over the course of several weeks, beginning on September 18, 2001 (after the September 11, 2001 attacks). Letters containing anthrax bacteria were mailed to several news media offices and two US Senators, killing five people.

Of the three types of non - conventional weapons - chemical, biological, or radioactive - chemical agents are the most accessible to terrorists. Information on how to prepare chemical-warfare agents is freely available from variety of open sources including the internet. It is also relatively easy to obtain dual use chemicals that can be used for terror attacks. Also the effects of chemical agents are immediate and therefore more suitable for the terrorists cause.

3.4.2 Reasonable worst-case scenario

Worst-case scenario would be difficult to define because the consequences of the attack will depend on several factors such as the location of the incident, weather conditions, mitigation activities and crowd density. However it reasonably safe to assume that worst-case scenario will be release of chemical agents in a close venue such as concert hall, train stations or ruffed football/sports stadium. The most famous CBRN attack is the Tokyo subway attack of 1995^{28 29}; a coordinated multiple terrorist attack in which the odourless, colourless, and highly toxic nerve gas sarin was released in the city's subway system. The attack resulted in the deaths of 13 people, and some 5,500 others were injured to varying degrees.

During the attack five men entered the Tokyo subway system, each with bags of sarin. Each boarded a separate subway line, their trains all headed toward the Tsukiji Station in central Tokyo. At virtually the same time, each attacker dropped his bags of sarin on the floor of the train and punctured them before exiting the train and station and leaving the scene in a waiting getaway car. As the liquid in the bags started to vaporize, the fumes began affecting the passengers. The trains continued on toward the center of the city, with sickened passengers leaving the cars at each station. The fumes were spread at each stop, either by emanating from the tainted cars themselves or through contact with liquid contaminating peoples' clothing and shoes. Many of the individuals who were overcome by exposure to sarin during the attack were those who came into contact with the agent while trying to assist those who already had been stricken.

²⁴ <https://www.theguardian.com/uk/2005/apr/14/terrorism.world2>

²⁵ <http://news.bbc.co.uk/2/hi/europe/1831511.stm>

²⁶ <http://www.nytimes.com/2002/08/19/world/qaeda-videos-seem-to-show-chemical-tests.html>

²⁷ <https://www.justice.gov/archive/amerithrax/docs/amx-investigative-summary2.pdf>

²⁸ https://www.huffingtonpost.com/2015/03/20/tokyo-subway-sarin-attack_n_6896754.html

²⁹ <https://www.britannica.com/event/Tokyo-subway-attack-of-1995>

3.4.3 Possible existing mitigations

CBRN attacks are extremely difficult to prevent since it is very easy to conceal the delivery means in innocent objects such as soft drinks cans (as in the Tokyo attacks) or other innocent looking containers. In open area events technological solutions are practically inefficient since detection sensors have limited range of detection. Mitigation in closed venues is also a challenge since existing detectors tend to produce large number of false alarms and that is the reason that to date they are widely used.

3.4.3.1 Chemical agents detectors

3.4.3.1.1 Description

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].

3.4.3.1.2 Possible effects on frequency and severity

Chemical agents' detectors can minimize the effect of potential attack by providing threat indication that may trigger evacuation of the public from the scene of the event by first responders [41]. The implementation of such technologies will probably won't deter or prevent terrorists from using that modus operandi since until activation they will remain undetected.

3.4.3.1.3 Potential adverse effects

Probably the main adverse effect of installation of CBRN detectors is the probability of false alarms that might lead to uncontrolled panic in the event of evacuation. False indications may also lead to cancellation of events and to great economic loss and reduction in public moral.

3.4.3.1.4 Stakeholders responsible for implementing the mitigation action

Stakeholders' responsibilities for implementing the action depend on the type of installation (e.g. permanent, temporary), the location (e.g. public or secluded area) and local regulations. These stakeholders typically include: local administrations, LEA, and event organizers

3.4.3.2 Training for detection of possible attacks

3.4.3.2.1 Description

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. The following signs may indicate the presence of a chemical weapon:

- breathing difficulties;
- uncontrollable coughing;

- runny nose;
- skin irritation;
- dizziness;
- fainting;
- strange odour;
- itchy/burning/watery eyes;
- small dead animals.

Trained security officers will be able to notice that several people are displaying those symptoms and commence response activities.

3.4.3.2.2 Possible effects on frequency and severity

The main effect of training will be the minimization of number of casualties and severity of injuries by shortening crowd exposure time to the chemical agent, prompt advice of the phenomena to the medical services, preparing them to the correct intervention and reducing the response time.

3.4.3.2.3 Potential adverse effects

Signs indicating possible chemical attack may appear in people who are not affected by chemical weapons, particularly in a crowded and poorly ventilated environment like a mass transit vehicle.

3.4.3.2.4 Stakeholders responsible for implementing the mitigation action

Stakeholders responsible for implementing the response activates typically include: LEA, fire department and medical teams.

3.5 COLD STEEL

3.5.1 Description of the risk

Given recent happenings, cold steel or knife attacks are a serious concern for LEAs in EU.

A cold steel or knife attack is an attack that does not concern any fire weapons and only bladed weapons are used. Many of this type of attacks have been happening recently due to the ease of obtaining a knife or other stabbing instrument compared to a fire weapon. It does not need any skills or instructions to use it, either. These attacks are also inexpensive, and very easy to carry out. Furthermore, they are more difficult to prevent for LEA's due to the lack of planning that they normally come with.

Europe has seen a big increase of this kind of attacks in the last ten years. Some of the most important - with high media impact - are:

- On 20 December 2014, a man near the city of Tours entered a police station and attacked several officers with a knife. He injured 3 people before he was shot and killed³⁰;
- On 26 July 2016, two terrorists attacked participants during a Mass at a Catholic church in Normandy. An 84-year-old priest was killed and four other people taken hostage³¹;

³⁰<https://www.telegraph.co.uk/news/worldnews/europe/france/11305974/French-police-shoot-dead-knifeman-who-was-shouting-Islamic-slogans.html>

³¹ <http://www.bbc.co.uk/news/world-europe-36892785>

- On 7 January 2016, a man wearing a fake explosive belt (a recurring element) attacked many police officers. The event is considered a failed attack since it did not carry any victims³²;
- On 18 July 2016, an underage man injured four people with a knife on a train near Würzburg, in Germany³³;
- On 22 March 2017, a combined attack finishing with a knife stabbing happened near the Palace of Westminster, in London. The terrorist drove a car into pedestrians first, and then tried to stab police officers and authorities in the palace Yard³⁴;
- On 3 June 2017, another van attack combined with stab attacks happened in London. Eight people died and 48 were injured³⁵;
- On 1 October 2017, a man killed two women in Marseille using a knife³⁶.

3.5.2 Reasonable worst-case scenario

Most of the worst attacks happening in Europe and concerning bladed weapons are combined with other kind of attacks, in which the stabbing is the last part. This action becomes as a last resort when the previous actions of the event fail or end, trying to kill and injure as many additional people as possible. A clear example is the Westminster attack. A man drove a car into pedestrians along the south side of Westminster Bridge and Bridge Street. He injured more than fifty people, and killed five. The car was crashed and the dropped off carrying a knife, trying to kill with it as many people as possible while running into New Palace Yard. He was able to fatally stab a police officer before being shot and dying. The attack becomes more difficult to stop when it is executed by a group of terrorist carrying knives, like in June 2017 London Bridge Attack, where three terrorists committed a knife attack after their van crashed. In this case, the attackers were able to stab four people [42]. Terrorists normally carry some other accessory threats, like fake explosive vests to make people more scared and prevent civilians to stop them. So reasonable worst-case scenarios adapted to mass gathering events could be:

- Attackers start with an additional action, like arriving with a vehicle and crashing it, or exploding a bomb somewhere close to the event;
- Attackers work in groups, with three, four or five armed people;
- Each terrorist carries a knife and move to a different position of the mass gathering and stab randomly as much people as possible;
- Terrorists stabbing the crowd and wearing explosive life vests (that can be fake).

3.5.3 Possible existing mitigations

3.5.3.1 Security checks and metal detectors at the event entrances

³² <https://www.wsj.com/articles/french-police-shoot-man-who-tried-to-enter-paris-police-station-1452169931>

³³ <http://www.bbc.com/news/world-europe-36827725>

³⁴ <http://nationalpost.com/news/world/several-injured-outside-british-parliament-house-on-lockdown-amid-reports-of-several-injuries-outside>

³⁵ <http://www.bbc.com/news/uk-40148737>

³⁶ <http://metro.co.uk/2017/10/01/man-shot-after-attacking-people-with-knife-at-train-station-in-marseille-6969015/>

3.5.3.1.1 Description

Adding security controls and checks at event entry points. Police will check people entering the event and metal detectors will be placed for the bags checking.

3.5.3.1.2 Possible effects on frequency and severity

Security checks (body search) and metal detectors are likely to considerably reduce frequency and severity of a cold steel attack. These measures allow the identification of weapons and they can work as deterrence for potential attackers.

3.5.3.1.3 Possible adverse effects

Security checks can slow down the entrance to the event venue causing queues in the access points. Moreover, having a heavier police presence can be uncomfortable for many civilians and many people can feel nervous and uncomfortable when asked to undergo security checks.

3.5.3.1.4 Responsible stakeholders for the implementation

LEAs are responsible for the event security controls.

3.5.3.2 Security officers inside the mass

3.5.3.2.1 Description

Setting different officers in strategic points inside the crowd to check for anomalies and being able to react as soon as possible. Security officers have to be trained in identifying and recognising suspicious signs.

3.5.3.2.2 Possible effects on frequency and severity

Deploying a number of security officers inside the crowd attending an event can reduce the frequency of the attack, since they can act as “human sensors” detecting anomalies and suspicious activities on the ground. They can promptly report the anomalies to the control command center asking for support and specific actions to be carried out.

3.5.3.2.3 Possible adverse effects

The measure requires additional trained workforce, increasing costs. Moreover, having a heavier police presence can be uncomfortable for many civilians and many people can feel nervous and uncomfortable.

3.5.3.2.4 Responsible stakeholders for the implementation:

Stakeholders responsible for implementing the response activates typically include: LEAs and the other stakeholders that are part of the control command centre on the ground (e.g. medical services, fire fighters, civil protection, etc.).

3.6 HIJACKING OF SOCIAL NETWORKS

3.6.1 Description of the risk

Social Networks (SNs) have become an extremely useful support to manage emergencies and large events. They are used to:

- engage in ongoing collaborative communications with community members and better prepare them for emergencies; and

- provide real-time emergency information to the event's participants.

In Europe many LEAs are using SN to diffuse information to citizens (in many cases also during events or emergencies): e.g. the Twitter[®] accounts of the London Police³⁷ or the *Ayuntamiento de Madrid*³⁸, the Facebook[®] pages of the *Polizia di Stato*³⁹ in Italy and the *Belgian Federal Politie*⁴⁰, just to give few examples.

Moreover, Facebook has also activated the so-called Safety Check, a crisis response tool to tell friends you're safe if you're in the affected area, and check to see if they're safe too. This tool has been widely used during, for example, the recent Paris and Brussels terroristic attacks to “connect” people in the affected areas and parents/relatives at home. However, the malicious use of Social Networks has been considered by many stakeholders as a serious threat as reported by Lindsey [43]: “Another concern is that some individuals or organizations might intentionally provide inaccurate information to confuse, disrupt, or otherwise thwart response efforts. Malicious use of social media during an incident could range from mischievous pranks to acts of terrorism. One tactic that has been used by terrorists involves the use of a secondary attack after an initial attack to kill and injure first responders. Social media could be used as a tool for such purposes by issuing calls for assistance to an area, or notifying officials of a false hazard or threat that requires a response. When using social media for situational awareness and response efforts, officials and first responders should be aware it could be used for malicious purposes and develop measures to mitigate those possibilities. If malicious use of social media during emergencies and disasters becomes problematic, Congress could elect the use of civil or criminal sanctions against individuals and organizations that purposely misuse social media with misleading information”.

Similar conclusions are reached by Wybo in [44] “the intrusion of social media in existing organizations raises a number of concerns: how to cope with new and time-consuming duties, how to avoid malicious use, and how to extract relevant information in the huge amount of data flowing through social media, knowing that most of them are just noise”.

3.6.2 Reasonable worst-case scenario

A clear example of how misuse of SNs can impact mass gathering events and, more in general, management of emergencies is what happened during Sandy hurricane and Boston Marathon bombing:

- during the Sandy hurricane storm of fake news and photos have been published on SNs: rumors, misleading or altered photos, sharing of untrue stories, and false alarms or unsubstantiated requests for help/support [45];
- tweets reporting fake deaths or promoting fake donation campaigns spread uncontrolled in the aftermath of the Boston Marathon bombing [46].

So reasonable worst-case scenarios adapted to mass gathering events are based on the idea that SNs could be exploited by terrorists to influence crowd during the event (e.g. force the crowd to concentrate in a

³⁷ <https://twitter.com/metpoliceuk>

³⁸ <https://twitter.com/MADRID>

³⁹ <https://www.facebook.com/poliziadistato.it/>

⁴⁰ <https://www.facebook.com/BelgianFederalPolice/>

place where a bomb is placed to increase the number of victims). The possible threats that could be imagined are:

- typically, people participating to mass gathering events are also following in real time SNs (e.g. the official Facebook page of the event or the Twitter page of an event-related influencer): this is particularly true when dealing with events involving young generations. These pages, if hijacked, could be used by terrorists [47] to put in practice a so-called “**psyber**” operation, i.e. “an operation in which terrorists could manipulate mass public emotion to create this effect that causes individuals or masses of people to spontaneously move in specific ways in response to messaging”;
- a recent phenomenon is the so-called **crowd-turfing**: as described in [48], crowd-turfing is a combination of “crowdsourcing” meaning recruiting large numbers of people to contribute a small effort each toward a big task (like labelling photos), and “astroturfing” meaning false grassroots support (in the form of bogus reviews or comments, for example). Crowd-turfing has been described well also in [49] and crowd-turfing systems are defined as: “systems where customers initiate “campaigns”, and a significant number of users obtain financial compensation in exchange for performing simple “tasks” that go against accepted user policies”. Crowd-turfing systems are widely active in China and are currently use mainly to generate fake news [48]. However, terrorists could exploit these systems to diffuse fake news through the social media of the event’s organizer or of the local LEA to control crowds;
- recently, crowd-turfing have evolved towards **automated crowd-turfing** systems [50], leveraging on deep learning language models to automate the generation of fake online reviews for products and services.

3.6.3 Possible existing mitigations

3.6.3.1 Description

Possible existing mitigations are:

- **Improving the security of access to SNs** to reduce the risk of compromised accounts through the protection of social media platforms, sites, profiles and accounts at the technical or system level (e.g. introducing encryption, two-factors authentication mechanisms, etc.).
- **Creating awareness on the use of trusted SN channels** by diffusing, together with the event dissemination material, the links to official SN channels. This is confirmed by the key findings of the H2020 MEDI@4SEC project⁴¹ in Deliverable D2.4 [51]:
 - The key requirement is to have a reliable and credible point of contact via social media so official accounts for government, event organisers and LEAs are needed;
 - For LEAs, a key requirement is training for their relevant staff in communication skills and expertise in the use, management and analysis of social media;

⁴¹ <http://media4sec.eu>

- Event organisers can use social media to directly collaborate with LEAs to ensure security and that order is upheld, directly report any security or safety incidents, seek advice and guidance on designing the event with a minimum level of security in mind to protect participants.
- **Identify trusted channels also for cultural minorities** (e.g. the Latinos community in U.S.A. as described in [52] requires communications from sources trusted by their community);
- **Counteract the spread of misinformation** and ensure participants were kept up to date with accurate information using more secure communication tools;
- **Crowd-turfing can be mitigated by the use of automated crawling systems** that are able to identify fake messages: example are those described by Zhao in [53] using machine learning and in [50] using automated classifiers based on Recurrent Neural Networks.

3.6.3.2 Possible effects on frequency and severity & Possible adverse effects

It is extremely difficult to describe possible effects on frequency and severity as well as the potential adverse effects of the proposed mitigation actions against misuse of SNs for the following reasons:

- there are no sufficient data on successful awareness campaigns on the use of SNs for mass gathering events, even if, as stated above, having a reliable and credible point of contact via social media is felt as a key requirement for both LEAs and events' organisers;
- detection of crowd-turfing activities is still at the research level, even if proposed approaches are claiming at 90-95% accuracy.

3.6.3.3 Responsible stakeholders for the implementation

Regarding the stakeholders responsible for implementing the mitigation action, it is possible to identify them as follows:

- improvement of the security of access to SNs: this is mostly left to the SN service providers and role of LEAs and event organisers is clearly limited;
- awareness campaigns on the use of official SN channels can be implemented by both LEAs and event organisers;
- detection of malicious use of SNs is a task that is still at the research level and therefore can be implemented only by IT centres managed by LEAs.

3.7 SHOOTING ATTACK

3.7.1 Description of the risk

Shooting attacks is one of the most common modus operandi used by terrorists. The relative ease availability of firearms in many parts of the world (through legal purchase, self-manufacturing, purchase from criminals, smuggle or theft from arsenals or private citizens) is one of the main causes that they are often used in terror attacks. Furthermore, unlike other terrorist means – such as IEDs or suicide vests – the use of firearms doesn't require special technical skills and access to highly regulated materials (used to assemble explosive devices). Attack with firearms can cause multiple casualties even if the shooter is untrained.

Throughout modern history there are numerous examples of terror shooting attacks; the weapon of choice in many of these attacks is the submachine gun or military grade assault rifle (such as the Russian made AK 47⁴²) due to their rapid-fire rate and amount of bullets in a single magazine (27 – 35 bullets in magazine⁴³).

In recent years the number of mass shooting incidents has been increased significantly. Many of these attacks - such as the attack Westgate mall attack⁴⁴, Kenya 2013 - were combined with activation of explosive devices or suicide bombers.

3.7.2 Reasonable worst-case scenario

Two of the worst shooting terror attacks targeted mass gathering events resulted in an extremely high death toll. The Las Vegas attack: on the evening of October 1, 2017⁴⁵, a gunman opened fire on a crowd of 22,000 people at the Harvest music festival on the Las Vegas Strip in Nevada. As a result of the attack 58 people died and 851 injured. Between 10:05 and 10:15 p.m. 64-year-old Stephen Paddock of Mesquite, Nevada, fired more than 1,100 rounds from his suite on the 32nd floor of the nearby Mandalay Bay hotel. About an hour after he fired his last shot into the crowd, he was found dead in his room from a self-inflicted gunshot wound. His motive remains unknown.

Another significant mass shooting terror attack is the attack on the Bataclan concert hall occurred on 13 November 2015⁴⁶. At approx. 21:40, a black Volkswagen Polo pulled up outside the venue and three heavily armed gunmen got out. The gunmen entered the building through the main entrance about 30-45 minutes after rock group the Eagles of Death Metal had begun their performance. Once in the building, they opened fire into the crowd. At around 10pm, the attackers took as many as 100 music fans hostage and a hostage situation had been declared. At around 12:20 am, security forces entered the hall. The siege came to an end when police shot one gunman, causing his suicide belt to blow up, before the other two attackers detonated theirs. The attacks claimed the lives of 130 people, injuring 352 others.

3.7.3 Possible existing mitigations

Shooting attacks can be mitigated in a variety of ways although experience has shown that a determined attacker can overcome most mitigations and inflict some damage.

3.7.3.1 Body search

3.7.3.1.1 Description

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 belongings of the visitors for further inspection (done manually or using scanning machines).

⁴² <https://www.britannica.com/technology/AK-47>

⁴³ <https://www.britannica.com/technology/AK-47>

⁴⁴ <https://www.theguardian.com/world/2013/oct/04/westgate-mall-attacks-kenya>

⁴⁵ <https://www.telegraph.co.uk/news/2017/10/02/las-vegas-strip-shooting-multiple-casualties-reported-near-mandalay/>

⁴⁶ <http://www.bbc.com/news/world-europe-34818994>

3.7.3.1.2 Possible effects on frequency and severity

Body search is likely to reduce frequency and severity considerably since it very effective tool in identification of weapons and also serves as very strong deterrence for potential attackers.

The method is also very beneficial in deterring from bringing to the event other counterparts (such as alcohol) forbidden by authorities or event organizers.

3.7.3.1.3 Potential adverse effects

There are two main adverse effects to using the body search method. The first one is that many people are feeling nervous and uncomfortable when asked to undergo body search. Although such practice is widely accepted in airports for example it is still uncommon in most mass gathering events (beside football games in some countries).

Additional adverse effect is because body search is relatively slow process that might cause ques in the access points to the event and therefore lead to a potential vulnerability (due to crowding of people in none sterile area).

3.7.3.1.4 Stakeholders responsible for implementing the mitigation action

Stakeholders responsible for implementing the action typically include: venue security staff and event organizers.

3.7.3.2 Walkthrough metal detector (WTMD)

3.7.3.2.1 Description

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.

3.7.3.2.2 Possible effects on frequency and severity

Walkthrough metal detectors are likely to reduce frequency and severity considerably since it very effective tool in identification of weapons and also serve as very strong deterrence for potential attackers.

3.7.3.2.3 Potential adverse effects

The single most important potential adverse effect when using WTMD is that the screening process is relatively slow – depending on level of calibration and sensitivity – due to the fact that the people are asked to remove metallic objects such as belts, jewellery and sometimes even shoes.

These may lead to formation of large queues and may require event organizers to open access point's wellhead of the event.

3.7.3.2.4 Stakeholders responsible for implementing the mitigation action

Stakeholders responsible for implementing the action typically include: venue security staff and event organizers.

3.7.3.3 X-ray scanning machine

3.7.3.3.1 Description

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.

An X-ray machine produces a controlled beam of radiation, which is used to create an image of the inside of the scanned object. This beam is directed at the area being examined. After passing through the object, the beam falls on a piece of film or a special plate where it casts a type of shadow. Different materials inside the luggage block or absorb the radiation differently. Dense objects blocks most of the radiation and appears white on the film. Less dense objects blocks less radiation and appear darker on the film. Often multiple images are taken from different angles so a more complete view of the area is available. The images obtained during X-ray scene are put through a process called “digitizing” so that they can be viewed on a computer screen.

3.7.3.3.2 Possible effects on frequency and severity

X-ray scanners are likely to reduce frequency and severity considerably since it very effective tool in identification of weapons and explosives and also serve as very strong deterrence for potential attackers.

3.7.3.3.3 Potential adverse effects

The main adverse effect when using X-ray machines is that the screening process may be delayed when closer exam is required for suspicious objects identified – depending on level of calibration and sensitivity – due to the fact the people are asked to remove metallic objects such as belts, jewellery and sometimes even shoes. These may lead to formation of large queues and may require event organizers to open access point's wellhead of the event.

3.7.3.3.4 Stakeholders responsible for implementing the mitigation action

Stakeholders responsible for implementing the action typically include: venue security staff and event organizers.

3.7.3.4 Training for identification of suspicious signs in behaviour and appearance

3.7.3.4.1 Description

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. Perquisite to such capabilities is that the security personnel will undergo specialized training in identification of suspicious signs. Abnormal behaviours of individuals, groups and crowds can be classified into different types: behaviour, body language, movement, and appearance indicators [54]. It is imperative to note that circumstance and context are critical to the interpretation of abnormal behaviour. Elements such as the cultural background, location, time, etc. plays crucial role in the classification of any behaviour as abnormal or suspicious. For example, an individual wearing raincoat walking in the street will not arouse suspicious in the wintertime but the same person wearing a rain coat in sunny summer day approaching big concert will raise suspicions.

3.7.3.4.2 Possible effects on frequency and severity

Past experience has shown that terror attacks, criminal activities and public disorder can be detected and thwarted by observing and identifying indicators of abnormal & suspicious behaviours⁴⁷.

3.7.3.4.3 Potential adverse effects

The main adverse effect may be the tendency to classify people from different background, ethnicity or culture as suspicious. What might be the norm in one culture may be perceived as anomalous behaviour in a different culture [55].

3.7.3.4.4 Stakeholders responsible for implementing the mitigation action

Stakeholders responsible for implementing the action typically include: venue security staff and event organizers.

3.8 POSSIBLE ADDITIONAL MITIGATIONS RESULTING FROM THE WORK IN LETSCROWD AND RESEARCH

Within the framework of LETSCROWD, other possible mitigation actions - linked to the tools developed in the project and other outcomes (e.g. training) - could be identified, contributing to the prevention and minimization of the security threats described in D3.2 [1] and discussed in the sections above. Such LETSCROWD additional mitigations are summarized in the Table 4, together with other ones resulting from the current research in the domain (when available).

Moreover, the table below (Table 3) maps the LETSCROWD contributions with regards both to the different stages to assess risk for mass gathering events (i.e. SRA for the early planning; DRA for the pre-event phase, see Table 3) (first part of the table), and the attack modes described in the previous sections (second part of the table).

Table 3: Mapping among LETSCROWD contributions, risk assessment stages and attack modes

LETSCROWD contributions						
	WP3	WP4	WP5 ⁴⁸			WP7
	DYNAMIC RISK ASSESSMENT METHODOLOGY (DRA)	POLICY MAKING TOOLKIT (PMT)	CROWD MODELLING TOOL (CMP)	HUMAN COMPUTER VISION TOOL (HCV)	SEMANTIC INTELLIGENCE TOOL (SIE)	TRAINING PACKAGE (LTP)
RISK ASSESSMENT STAGES						
SRA (Early planning)		✓	✓			✓
DRA (Pre – event)	✓			✓	✓	

⁴⁷<http://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Port-and-Facility-Compliance-CG-FAC/Americas-Waterway-Watch/>

⁴⁸ The innovative communication guidelines (ICP) are not included in this table. They offer strategies to communicate with the crowd and they can be applied to mitigate hazards generated by the crowd that will be explored in the next version of the deliverable (D5.6).

ATTACK MODE						
Vehicle used as weapon			✓			
Package Type IED			✓	✓		✓
Vehicle-borne IEDs (VBIEDs)			✓	✓		✓
Suicide bomb IED	✓		✓	✓		✓
CBRN attack			✓			
Cold steel		✓		✓		✓
Hijacking of social networks					✓	
Shooting			✓		✓	✓

Table 4: Possible additional mitigations resulting from LETSCROWD and research

Attack mode	LETSCROWD mitigations	Other mitigations from research
Vehicle used as weapon (vehicle ramming)	Crowd Modelling Tool⁴⁹ (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.	A number of companies are exploring ways to enhance advanced emergency braking (AEB) systems, which engage a vehicle's brakes when sensors in the vehicle detect a collision. Such technology has been mandatory in new heavy vehicles since 2014 under EU law, and enhancing the technology to stop the vehicle immediately, and expanding its use in all vehicles, would surely prevent a number of vehicle-ramming attacks. Still, a savvy terrorist could simply use an older vehicle or find a way to disable the AEB system. Other companies have looked towards "geo-fencing" technology that would create a digital force field that can slow down unauthorized vehicles and eventually bring them to a halt.

⁴⁹ For almost all the security threats discussed, the *crowd modelling tool* (including the GIS technology) 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.

IEDs 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 recognizing suspicious activities, and providing immediate and proper emergency responses to suspicious items and patterns (identified in [56]).

Human-Centred Computer vision tools (D5.4 – M12 and D5.8 – M24). They can help to detect abandoned objects in the mass gathering venue. However, it is a challenging computer vision task, requiring a high-level understanding of a scene.

Vehicle-borne IEDs (VBIEDs)

Crowd Modelling Tool. See above (package type).

LEAs training package. See above (package type).

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.

(Squad of) Suicide bomb IED

LEAs training package; Crowd Modelling Tool; and Human-Centred Computer vision tools. LETSCROWD

There are new methods to detect bombs that could be applied to mass gathering security to better detect a

is studying crowd behaviours to help identify terrorists and suspicious behaviours, some of which could be 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 automate camera detection, where crowd simulations will forecast “normal” situations and be used to train the camera to detect “abnormal situations”.

suicide bomb on a person, for example infrared detection at a distance [57].

Dynamic risks assessment for mass-gathering (D3.2 and D3.6 – M20). In general, the gathering of weak signals identified by the proposals in D3.2 for dynamic risk assessment can combine to increase the likelihood that a suicide bomber is detected before a detonation: there are several possible indicators that may suggest the preparation of a suicide bombing. Before the Manchester attacks, the attacker was seen “scoping” the venue before the event, which could be detected in dynamic risk assessment as a weak signal.

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.

Cold steel (e.g. stabbing)	<p>Policy making toolkit (D4.4 – M12 and D4.8 – M24) will help preventing attacks from a poorly chosen venue or time.</p> <p>LEAs training package. Thanks to LEAs' training and human behaviour investigation, officers will improve their ability and skills to detect anomalous human behaviour patterns.</p> <p>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.</p>	
Hijacking of social networks	<p>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.</p>	<p>The aspect of detecting fake news in real-time is one of the themes at the forefront of the research in the SN areas. A real-time detection of fake news could help to mitigate their effects and impacts by shutting them down before fake news are too widely diffused. Examples of this research are the works of Farajtabar [58] and Zhao [50], [53] on real-time fake news mitigation.</p>
Shooting	<p>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.</p> <p>LEAs training package designed to enhance capabilities of police officers in identification of suspicious signs in behaviour and appearance.</p> <p>Semantic intelligence applied to social networks and 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.</p>	

4 Conclusions and next steps

The D3.3 aims at proposing an overview of the current soft and hard solutions usable to mitigate the vulnerabilities and threats identified in D3.2. The document is the first version of the report on soft and

hard mitigation actions. It includes the concept of mitigation action within the risk management framework, taking into account the risk treatment phase. Mitigations have been described referring to the possible effects on frequency and severity; the potential adverse effects and the stakeholders responsible for implementing the mitigation action. Mitigations proposed in the document arise from the literature. They are generic and not universal, and they have to be selected on the basis of the characteristics of the event under analysis. Other mitigation actions came out from the work carried out in LETSCROWD. They consist of contributions that the project can provide to the different terrorism attack modes including both project technological solutions (e.g. tools like: crowd modelling, semantic intelligence, human computer vision, policy making toolkit) and methodologies (e.g. Dynamic risk assessment). The mitigations proposed – from the literature review and from the LETSCROWD project - refer to the event preparation phase (i.e. early planning and pre-event).

The second version of the deliverable (D3.7) will explore the following aspects:

- **LEAs' mitigation strategies review.** Given that this document offers mitigation actions coming from the literature review, an operational perspective from LEAs mitigation practices is still missing. The next version of the deliverable will include it, together with an analysis of LEAs' needs and gaps concerning the mitigation strategies currently applied;
- **mitigations referring to hazards generated by the crowd** as a consequence of a security threat (possible cascade effects). These types of hazards might be mitigated taking into account other LETSCROWD outcomes. For instance, the Innovative communication guidelines (D5.2 – M12 and D5.6 – M24) will offer strategies to communicate with the crowd, improving security operators and first responders' communication skills and competences both in the pre-event and execution phases (especially in case of emergency).

5 REFERENCES AND ACRONYMS

5.1 REFERENCES

- [1] LETS-CROWD project. , “Deliverable D3.2 LETSCROWD Progress report on dynamic risks for mass gatherings.” 2018.
- [2] International Organization for Standardization, *ISO 31000 Risk management — Principles and guidelines*, 2009.
- [3] Center for the Protection of National Infrastructures (CPNI), “Protecting Crowded Places: Design and Technical Issues,” 2012. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97992/design-tech-issues.pdf.
- [4] Counter Extremism Project (CEP), “Vehicles as Weapons of Terror,” 2018. [Online]. Available: <https://www.counterextremism.com/vehicles-as-weapons-of-terror#dd-conclusion>.
- [5] M. S. Neiberg, ““No More Elsewhere”: France Faces the New Wave of Terrorism.”,” *The Washington Quarterly* 40.1, 2017.

- [6] Department of Defense (DOD) – US Army Corps of Engineers, “ Anti-Ram Vehicle Barrier List,” 2018. [Online]. Available: <http://dodantiramlist.com/2018>.
- [7] Center for the Protection of National Infrastructures (CPNI), “Hostile Vehicle Mitigation,” 2017. [Online]. Available: <http://www.cpni.gov.uk/hostile-vehicle-mitigation> .
- [8] National Counter Terrorism Security Office (NaCTSO), “Crowded Places Guidance,” 2017. [Online]. Available: <https://www.gov.uk/government/collections/crowded-places>.
- [9] International Organisation for Standardization, IWA 14-1:2013 Vehicle security barriers, Part 1: Performance requirement, vehicle impact test method and performance rating, 2013.
- [10] International Organisation for Standardization, IWA 14-2:2013 Vehicle security barriers , Part 2: Application, 2013.
- [11] British Standards Institution, PAS 68:2013, “Impact test specifications for vehicle security barrier systems,” 2013.
- [12] British Standards Institution, PAS 69:2013 , “Guidance for the selection, installation and use of vehicle security barrier systems,” 2013.
- [13] R. Tait, *Israeli woman and soldier killed in twin stabbing attacks*, The Daily Telegraph, 2014.
- [14] S. Garfield, *Terrorists are foiled at Glasgow airport*, The Guardian, 2007.
- [15] Department for Transport, “Impact of hostile vehicle mitigation measures (bollards) on pedestrian crowd movement,” 2013. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/565788/impact-bollards-crowd-movement-research-report-1.pdf.
- [16] Department for Transport, “Impact of hostile vehicle mitigation measures (bollards) on pedestrian crowd movement: phase 2,” 2014. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/565789/impact-bollards-crowd-movement-research-report-2.pdf.
- [17] Department for Transport, “Influence of bollards on pedestrian evacuation flow,” 2016. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/650628/tal-1-16-influence-of-bollards.pdf.
- [18] Center for the Protection of National Infrastructures (CPNI), “Resilient Design Tool for Counter Terrorism,” 2012. [Online]. Available: <http://www.securedbydesign.com/wp-content/uploads/2014/02/resilient-design-tool-for-counter-terrorism.pdf>.
- [19] Federal Bureau of Investigation, “Terrorist Use of Vehicle Ramming Tactics,” 2012. [Online]. Available: <https://publicintelligence.net/ufouo-dhs-fbi-warning-terrorist-use-of-vehicle-ramming-tactics/>.
- [20] Transportation Security Administration, “Vehicle Ramming Attacks: Threat, Landscape, Indicators and Countermeasures,” [Online]. Available: <https://info.publicintelligence.net/TSA-VehicleRamming.pdf>.
- [21] G4S Canada, “Vehicular Terrorism: The Threat Behind the Wheel,” [Online]. Available: http://www.g4s.ca/-/media/g4s/canada/files/whitepapers/usa/vehicular_terrorism_the_threat_behind_the_wheel.as

hx.

- [22 A. Pasquini, S. Pozzi, L. Save, A. M. Sujan, Requisites for successful incident reporting in resilient organisations, Resilience engineering in practice: a guidebook, Farnham, Surrey, England, 2011.
- [23 Department of Defense Dictionary of Military and Associated Terms, JointPublication1-02, 2001.
- [24 Australia- New Zeland counter terrorism committee, “Australia- New Zeland counter terrorism committee,” 2017. [Online]. Available: <https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/IED-Guidelines/IED-guidelines-crowded-places.pdf>.
- [25 Wehri, Matthew T., “Preventing an Improvised Explosive Device (IED) terror campaign in the United States,” 2007. [Online]. Available: https://calhoun.nps.edu/bitstream/handle/10945/3029/07Dec_Wehri.pdf?sequence=1.
- [26 Action On Armed Violence, AOAV, “Improvised Explosive Device (IED) Monitor,” 2017. [Online]. Available: <https://reliefweb.int/sites/reliefweb.int/files/resources/IED-Monitor-Report-for-web-final.pdf>.
- [27 Federal Emergency Management Agency, “Design considerations,” [Online]. Available: https://www.fema.gov/media-library-data/20130726-1624-20490-7003/430_ch2.pdf.
- [28 Cambridge Dictionary, 2018. [Online]. Available: <https://dictionary.cambridge.org/dictionary/english/suicide-bomber#>.
- [29 The Atlantic, ““The Logic of Suicide Terrorism”,” 2003. [Online]. Available: <https://www.theatlantic.com/magazine/archive/2003/06/the-logic-of-suicide-terrorism/302739/>.
- [30 M. M. Hafez, *Suicide Bombers in Iraq: The Strategy and Ideology of Martyrdom*, 2007.
- [31 R. A. PAPE, *The strategic Logic of Suicide Terrorism*, 2005.
- [32 L. de la Corte Ibáñez, “The Social Psychology of Suicide Terrorism,” 2014. [Online]. Available: <https://www.naija.ng/882358-shocking-250-people-die-worst-suicide-bombing-ever-photos.html#882358>.
- [33 BBC News, “Manchester attack: Extradition bid for Salman Abedi's brother,” 2017. [Online]. Available: <http://www.bbc.co.uk/news/uk-england-manchester-41839277>.
- [34 Reuters Staff, “Timeline of Paris attacks according to public prosecutor,” 2016. [Online]. Available: <https://www.reuters.com/article/us-france-shooting-timeline/timeline-of-paris-attacks-according-to-public-prosecutor-idUSKCN0T31BS20151114>.
- [35 O Hakeem, “Worst suicide bombing ever, as number of deaths rises to 250,” 2017. [Online]. Available: <https://www.naija.ng/882358-shocking-250-people-die-worst-suicide-bombing-ever-photos.html#882358>.
- [36 Office for Bombing Prevention, “Counter-IED resources guide,” 2017. [Online]. Available: <https://www.dhs.gov/sites/default/files/publications/obp-counter-ied-resources-guide.pdf>.
- [37 Technical resource for incident prevention , “Vehicle Borne IED identification guide,” [Online]. Available: <https://www.fbiic.gov/public/2008/oct/DHSVehicleBorneIEDIdentificationGuideParkedVehicles.pdf>.

- [38 NaCTSO, "Counter Terrorism Protective Security Advice for Major Events," 2016. [Online].
] Available: http://www.ukcma.com/wp-content/uploads/2016/06/Major_Events_Reviewed.pdf.
- [39 Home Office, "Crowded Places: The Planning System and Counter-Terrorism," 2012. [Online].
] Available:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/375208/Crowded_Places-Planning_System-Jan_2012.pdf.
- [40 *Counter Terrorism Chemical Detector for Transit Vehicles*, IDEA Project 40, 2005.
]
- [41 *Guide for the Selection of Chemical Detection Equipment for Emergency First Responders*,
] DHS, 2007.
- [42 BBC, "news, London Bridge attack," 05 June 2017. [Online]. Available:
] <http://www.bbc.com/news/uk-40148737>.
- [43 B. Lindsey, "Social Media and Disasters: Current Uses, Future Options, and Policy
] Considerations," U.S. Congressional Research Service, 2011.
- [44 J. Wybo, F. Fogelman-Soulié, G. Goultas, E. Freyssinet and P. Lions, "Impact of social media
] in security and crisis management: a review," *Int. J. Emergency Management*, vol. 11, no. 2, 2015.
- [45 A. Holpuch, "Hurricane Sandy brings storm of fake news and photos to New York," The
] Guardian, 30 October 2012. [Online]. Available: <https://www.theguardian.com/world/us-news-blog/2012/oct/30/hurricane-sandy-storm-new-york>.
- [46 A. Gupta, H. Lamba and P. Kumaraguru, "\$1.00 per RT #BostonMarathon #PrayForBoston:
] Analyzing Fake Content on Twitter," *IEEE eCrime Researchers Summit (eCRS)*, 2013.
- [47 P. Yannakogeorgos, "Rethinking the Threat of Cyberterrorism," in *Cyberterrorism
] Understanding, Assessment, and Response*, Springer, 2014.
- [48 S. Jacobs, "Fake Followers for Hire, and How to Spot Them," MIT Technology Review, 30
] June 2014. [Online]. Available: <https://www.technologyreview.com/s/528506/fake-followers-for-hire-and-how-to-spot-them/>.
- [49 G. Wang, C. Wilson, X. Zhao, Y. Zhu, M. Mohanlal, H. Zheng and B. Zhao, "Serf and Turf:
] Crowdturfing for Fun and Profit," in *Proceedings of the International World Wide Web Conference (WWW 2012)*, Paris, 2012.
- [50 Y. Yao, B. Viswanath, J. Cryan, H. Zheng and B. Zhao, "Automated Crowdturfing Attacks and
] Defenses in Online Review Systems," in *ACM Conference on Computer and Communications Security (CCS)*, Dallas, 2017.
- [51 MEDI@4SEC Project, "Deliverable 2.4: Workshop 2 Report: Riots & Mass Gatherings," 2017.
]
- [52 National Council of La Raza (NCLR), "Emergency Managers Tool Kit: Meeting the Needs of
] Latino Communities," 2011.
- [53 G. Wang, T. Wang, H. Zheng and B. Y. Zhao, "Man vs. Machine: Practical Adversarial
] Detection of Malicious Crowdsourcing Workers," in *Proceedings of the 23rd USENIX Security Symposium*, San Diego, CA, 2014.
- [54 International Maritime Organization, "Guide to Development and Implementing Suspicious
] Activity Identification Programs in Ports," 2015.

[55 Recommendation 2010/C 184 E/25, “Profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control,” 2009.

[56 LETS-CROWD project, “Deliverable 3.1 Progress report on models of patterns of human behaviours,” 2017.

[57 R. A. M. R. F. M. P. V. N. a. J. B. C. Kendziora, “Detecting traces of explosives,” [Online]. Available: <http://spie.org/newsroom/5835-detecting-traces-of-explosives?SSO=1>.

[58 M. Farajtabar, J. Yang, X. Ye, H. Xu, R. Trivedi, E. Khalil, S. Li, L. Song and H. Zha, “Fake News Mitigation via Point Process Based Intervention,” *arXiv.org*, vol. 1703.07823, 2017.

5.2 ACRONYMS

Acronyms List	
AOAV	Action on Armed Violence
CBRN	Chemical, biological, radiological, and nuclear
CMP	Crowd Modelling and Planning tool
CPTED	Crime Prevention through environmental design
CWA	Chemical Warfare Agents
DRA	Dynamic Risk Assessment
FEMA	Federal Emergency Management Agency
GIS	Geographic Information System
HCV	Human-Centred Computer Vision
ICP	Innovative Communication Procedures
IEDs	Improvised explosive devices
IT	Information Technology
LEA	Law Enforcement Agency
LTP	LEA Training Package
PMT	Policy Making Toolkit
SIE	Semantic Intelligence Engine
SNs	Social Networks
SRA	Static Risk Assessment
SVBIED	Suicide Vehicle Borne Improvised Explosive Device
TIC	Toxic Industrial Chemicals
VBIED	Vehicle Borne Improvised Explosive Device
WTMD	Walkthrough metal detector