



Title:	Document Version:
D3.2 Progress report on dynamic risks for mass gatherings	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*:
M10 (February 2018)	M10	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:
Carlo Dambra	PROPRS	WP3

#### Authors (organisation):

C. Dambra, A. Gralewski (PROPRS), C. Graf (RAILSEC), Y. Alon, C. Graf (RAILSEC), G. Fumera (UNICA), D. Ariu (PLURIBUS), H. Nitsch, S. Allertseder (BayFHVR), A.G. Silva (ESYS), C. Peres (ADM), J. A. Alonso Velasco (ERT), I. Jacobs, G. Smet (LPV), V. Da Silva Reis, P. Esteves Grilo (PSP), P. Townsend (CROWD)

#### Abstract:

This document represents a progress report on WP3 risk assessment, including identified vulnerabilities, threats and hazards, the related likelihoods and consequences and possible approaches to implement a methodology for static and dynamic risk assessment in mass gatherings. It will be the basis for deliverable D3.4.

#### Keywords:

Mass gathering, static risk assessment, risk assessment, dynamic risk assessment, crowd management, weak signal

## Revision History

Revision	Date	Description	Author (Organisation)
V0.01	08.01.2018	D3.2 Table of Content	C. Dambra (PROPRS)
V0.02	15.01.2018	Revised D3.2 ToC	C. Dambra (PROPRS)
V0.03	29.01.2018	First contributions	C. Dambra, A. Gralowski (PROPRS), G. Fumera (UNICA), D. Ariu (PLURIBUS), S. Allertseder (BayFHVR), A.G. Silva (ESYS), C. Peres (ADM), J. A. Alonso Velasco (ERT), Y. Alon, C. Graf (RAILSEC), I. Jacobs, G. Smet (LPV), V. Da Silva Reis, P. Esteves Grilo (PSP)
V0.04		First full draft	C. Dambra, A. Gralowski (PROPRS)
V0.05	06.02.2018	2 <sup>nd</sup> full draft for internal review	C. Dambra, A. Gralowski (PROPRS)
V0.06	17.02.2018	Version with comments from internal review (DBL and CROWD)	C. Dambra, A. Gralowski (PROPRS), P. Townsend (CROWD), A. Pasquini (DBL)
V0.07	27.02.2018	Final version for last checks	C. Dambra A. Gralowski (PROPRS)
V1.00	27.02.2018	Final version ready to be submitted to EC	C. Dambra A. Gralowski (PROPRS)



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 represents a progress report of the LETSCROWD approach to risk analysis of the public events assessment. It is based on ISO 31000 and 31010 standards and describes the steps required to prepare and execute such events.

The approach starts presenting an overview on risk assessment methodology according to ISO 31000 and how it is influenced by LETSCROWD topic. The overview covers the following aspects: risk criteria and system boundaries definition hazards/threats identification, probability and consequences evaluation, resulting risk calculation and finally risks reduction and/or mitigation.

The overview on risk assessment is followed by the analysis of the overall LETSCROWD requirements for risk assessment extracted from the European Security Model and from interviews with the LEAs in the project.

On the basis of the requirements, improvements to SRA risk assessment, by introduction of crowd modelling to model specific events such as evacuation, and business analytics for assessing and extracting knowledge from similar events which occurred in the past are presented.

Then, possible risk assessment techniques based on both qualitative and quantitative methods are described including Boston Square, fault and event trees, Bayesian approaches Monte Carlo and Fuzzy Logic techniques.

To better identify the most suitable approaches to Dynamic Risk Assessment (DRA), the threats faced by the public attending the event, e.g. terrorist, are discussed and how to represent them in DRA. The three phases for mass gathering events, pre-event, execution and post-event are described and key activities in each phase presented.

Finally, the report then introduces the idea of weak signals, its assessment, leading to understanding of possible terrorist threats, the technologies proposed to sense weak signals, their interaction and a method of assessing their impact in DRA.

The report concludes with the following recommendations for the implementation of a practical approach:

- The main threats of interest for LETSCROWD are those linked to terrorism including lone wolves and domestic extremisms, since the risks associated to clashes between different groups are already well known by LEAs and much more predictable in terms of dynamic behaviour.
- Given the above assumption, most of the risks to be considered are falling within the Low Probability High Impact category, thus making difficult to collect data on likelihoods and consequences.
- The Static Risk Assessment phase of the involved LEAs appears to be well structured according to standard principles of risk assessment and therefore it can be simply improved by introducing:
  - Crowd modelling to better assess consequences on participants;
  - Data analytics to improve the extraction of knowledge from databases of past events.
- The difficulty in collecting statistical evidence on the most critical threats makes the qualitative approaches more appropriate for the LETSCROWD Dynamic Risk Assessment, taking also into account the need to have the “man in the loop”.
- The most promising approach appears to be a situational awareness tool integrating:
  - Real-time GIS able to manage heterogeneous alerts.
  - A standardised protocol to handle risk-related geo- and time-referenced alerts.
  - A semi-automatic procedure to
    - Manage the alerts and evaluate how they dynamically contribute to the risk(s) for which they can be considered precursors.

- To display the most significant alerts to the operator to allow him to dynamically modify the levels of the different considered risks accordingly;
- Identify and show to the operator the most appropriate procedures to handle the new levels of risk.



## Index

<b>1</b>	<b>INTRODUCTION</b>	<b>10</b>
1.1	PURPOSE OF THE DOCUMENT	10
1.2	SCOPE OF THE DOCUMENT	10
1.3	STRUCTURE OF THE DOCUMENT	10
1.4	DEFINITIONS	10
<b>2</b>	<b>INTRODUCTION TO RISK ASSESSMENT</b>	<b>12</b>
2.1	INTRODUCTION	12
2.2	GENERAL RISK ASSESSMENT PROCEDURES	12
2.2.1	SYSTEM BOUNDARIES DEFINITION	13
2.2.2	RISK CRITERIA DEFINITION	13
2.2.3	POSTULATE SCENARIOS	13
2.2.4	IDENTIFY HAZARDS/THREATS	14
2.2.5	ASSESS PROBABILITIES/LIKELIHOOD	15
2.2.6	ASSESS CONSEQUENCES	15
2.2.7	ASSESS RISK	16
2.2.8	ASSESS RISK AGAINST CRITERIA	16
2.2.9	RISK REDUCTION/MITIGATION MEASURES AND RELATED PROCEDURES	16
<b>3</b>	<b>DYNAMIC RISK ASSESSMENT (DRA) REQUIREMENTS</b>	<b>18</b>
3.1	THE EUROPEAN SECURITY MODEL (ESM)	18
3.2	REQUIREMENTS FROM DELIVERABLE D2.2	18
3.3	FEEDBACK FROM VISIT TO LAW ENFORCEMENT AGENCIES (LEAs)	19
3.3.1	INTRODUCTION	19
3.3.2	SYNTHESIS OF THE VISITS TO LEAs	19
<b>4</b>	<b>IMPROVEMENTS TO STATIC RISK ASSESSMENT</b>	<b>21</b>
4.1	CROWD MODELLING	21
4.2	ANALYTICS ON EXISTING DATABASES	22
<b>5</b>	<b>POSSIBLE APPROACHES TO DYNAMIC RISK ASSESSMENT</b>	<b>23</b>
5.1	QUALITATIVE APPROACHES	23
5.1.1	HISTORICAL DATA COLLECTION	24
5.1.2	ELICITATION OF KNOWLEDGE FROM EXPERTS	24
5.1.3	FAULT TREE ANALYSIS	25
5.1.4	SITUATIONAL AWARENESS AND GEOGRAPHIC INFORMATION SYSTEMS	26
5.1.5	GEOREFERENCED TIME-STAMPED ALERTS	28
5.2	QUANTITATIVE APPROACHES	30
5.2.1	BAYESIAN NETWORKS (BNs)	31
5.2.2	PROBABILISTIC DECISION TREES (PDTs)	31

5.2.3	SIMULATIONS	33
5.2.4	MONTE CARLO SIMULATIONS	33
5.2.5	FUZZY LOGIC MODELS	34
5.3	CONCLUSIONS	35
<b>6</b>	<b>LETSCROWD APPROACH TO DYNAMIC RISK ASSESSMENT</b>	<b>36</b>
<b>6.1</b>	<b>THE RISKS CONSIDERED IN LETSCROWD</b>	<b>36</b>
6.1.1	THE RISKS AND RELATED THREATS	36
6.1.2	THE LIKELIHOOD OF THE THREATS	40
<b>6.2</b>	<b>THE DIFFERENT PHASES TO ASSESS RISKS FOR MASS GATHERING EVENTS</b>	<b>41</b>
6.2.1	EARLY PLANNING	42
6.2.2	PRE-EVENT	42
6.2.3	EVENT EXECUTION	45
6.2.4	EVENT CLOSING AND ASSESSMENT	46
<b>7</b>	<b>ANALYSIS OF EXISTING SENSED WEAK SIGNALS</b>	<b>47</b>
<b>7.1</b>	<b>CYBER THREATS INTELLIGENCE ON MASS GATHERING EVENTS</b>	<b>47</b>
7.1.1	WEAK SIGNALS FOR THE DIGITAL SCENARIO	49
7.1.2	WEAK SIGNALS FOR THE PHYSICAL SCENARIO	50
<b>7.2</b>	<b>SEMANTIC INTELLIGENCE</b>	<b>52</b>
7.2.1	SOCIAL NETWORKS AND POSSIBLE THREATS TO MASS GATHERINGS EVENTS	52
7.2.2	THE USE OF SEMANTIC INTELLIGENCE TO DETECT WEAK SIGNALS IN SOCIAL NETWORKS	53
7.2.3	INTERNET HARVESTING FOR LONE WOLF TERRORIST DETECTION	56
<b>7.3</b>	<b>HUMAN-CENTRED COMPUTER VISION</b>	<b>56</b>
7.3.1	CROWD DENSITY ESTIMATION	57
7.3.2	PATTERNS OF CROWD MOVEMENTS	57
7.3.3	SPECIFIC INDIVIDUALS OR GROUPS MOVING IN THE SCENE.	58
7.3.4	FORMATION OF GROUPS OF PEOPLE EXHIBITING HOMOGENEOUS CLOTHING APPEARANCE.	58
7.3.5	DETECTION AND BEHAVIOUR ANALYSIS OF VEHICLES IN THE SCENE.	58
7.3.6	DETECTION OF ABANDONED OBJECTS	58
<b>7.4</b>	<b>HUMAN AS SENSOR</b>	<b>59</b>
<b>7.5</b>	<b>RELATIONSHIPS BETWEEN WEAK SIGNALS AND MASS GATHERING THREATS</b>	<b>60</b>
7.5.1	RELATIONSHIP BETWEEN WEAK SIGNALS AND THREATS' PRECURSORS	60
7.5.2	WEAK SIGNALS INTERPRETATION	62
<b>8</b>	<b>WAY FORWARD IN LETSCROWD AND CONCLUSIONS</b>	<b>64</b>
<b>8.1</b>	<b>IMPLEMENTATION OF A PRACTICAL APPROACH</b>	<b>64</b>
<b>8.2</b>	<b>CONCLUSIONS</b>	<b>64</b>
<b>9</b>	<b>REFERENCES AND ACRONYMS</b>	<b>65</b>
<b>9.1</b>	<b>REFERENCES</b>	<b>65</b>
<b>9.2</b>	<b>ACRONYMS</b>	<b>68</b>
<b>10</b>	<b>APPENDIX 1 - EXAMPLE OF A SECURITY EVENT IN GERMANY</b>	<b>70</b>

<b>10.1</b>	<b>POLICE AND EVENTS</b>	<b>70</b>
<b>10.2</b>	<b>TASKS</b>	<b>70</b>
<b>10.3</b>	<b>DESCRIPTION OF POLICE ACTIVITIES</b>	<b>70</b>
10.3.1	BEFORE THE EVENT: PREPARATION	70
10.3.2	DURING THE EVENT: IMPLEMENTATION	70
10.3.3	FOLLOW-UP	71
<b>10.4</b>	<b>RISK ASSESSMENT</b>	<b>71</b>
<b>10.5</b>	<b>ROLE OF THE POLICE IN THE LICENSING PROCEDURE</b>	<b>71</b>
10.5.1	OBJECTIVES	71
10.5.2	LEGAL GROUNDS FOR POLICE INVOLVEMENT	71
10.5.3	FACTORS FOR SUCCESSFUL POLICE INVOLVEMENT	71
10.5.4	ORGANIZATIONAL STRUCTURE OF THE POLICE DURING AN EVENT	72
<b>10.6</b>	<b>PRESS AND PUBLIC RELATIONS</b>	<b>72</b>





## LIST OF FIGURES

Figure 2-1 - The standard ISO 31000 procedure and LETSCROWD aspects .....	12
Figure 4-1 - Example of crowd simulation from T5.1 .....	22
Figure 5-1 - Explosive evacuation distance .....	24
Figure 5-2 – Possible use of GIS-based tools (1).....	27
Figure 5-3 – Possible use of GIS-based tools (2).....	28
Figure 5-4 - The CAP alert message model.....	29
Figure 5-5 - A generic decision tree.....	32
Figure 5-6 - Unidentified left package in public place .....	32
Figure 5-7 - Monte Carlo simulation model .....	34
Figure 6-1 - The Static & Dynamic Risk Assessment stages.....	42
Figure 6-2 - The approach for the Pre-Event stage .....	43
Figure 6-3 – Pre-Event risk assessment steps .....	44
Figure 6-4 - Event Execution process.....	46
Figure 7-1 - Simplified view of the components comprising the semantic intelligence engine .....	53
Figure 7-2 - Lone wolf weak signal detection.....	56
Figure 7-3 - The patterns of crowd movements.....	57
Figure 7-4 - The UK Metropolitan Police suspicious activity report form .....	60

## LIST OF TABLES

Table 1 - Definitions.....	11
Table 2 - Example of a likelihood scale.....	15
Table 3 – Consequence table for the crowd.....	15
Table 4 – Consequence table for the organiser and the mass gathering.....	15
Table 5 - Example of a risk matrix (for each type of risk) .....	16
Table 6 - Example of Probability Density Functions (PDF) .....	25
Table 7 - IDS parameters for alert dangerousness .....	30
Table 8 - Example of LETSCROWD alert dangerousness parameters.....	30
Table 9 - Terrorist risk levels.....	37
Table 10 - Terrorist response level .....	37
Table 11 - Threats to mass gathering events .....	38
Table 12 - Threat/precursors table.....	40
Table 13 - The role of “Cyber” in the scenario .....	48
Table 14 - Categorisation produced by COGITO SW .....	54
Table 15 - Extract of the intelligence engine .....	55



Table 16 - Slang types .....	55
Table 17 - Output of the intelligence engine.....	56
Table 18 - Threat's precursor detection .....	61
Table 19 – Example of a sequence of correlated weak signals .....	63



## 1 INTRODUCTION

### 1.1 PURPOSE OF THE DOCUMENT

This document is the first version report on WP3 risk assessment, including identified vulnerabilities, threats and hazards, the related likelihoods and consequences and possible approaches to implement a methodology for static and dynamic risk assessment in mass gatherings.

### 1.2 SCOPE OF THE DOCUMENT

The scope of this document is:

- To introduce risk assessment and the LETSCROWD approach towards Dynamic Risk Assessment (DRA) to be consolidated in Deliverable D3.4.
- To provide an analysis of the problem of risk management for mass gathering events, highlighting the possible security threats to the crowd.
- To briefly propose improvements to the current practices for Static Risk Assessment (SRA).
- To analyse the weak signal detection methodologies introduced in LETSCROWD, relate them to the identified threats and to evaluate their potential detection capabilities.
- To suggest possible options for the design of the DRA methodology to be further developed in D3.4.

### 1.3 STRUCTURE OF THE DOCUMENT

The document is structured as follows:

- A brief description of the possible approaches to risk assessment is introduced in Section 2.
- Section 3 summarises the DRA requirements extracted from the European Security Model (ESM), the Deliverable D2.2 and from a series of interviews with the LEAs in the project.
- Section 4 proposes two possible improvements for the Static Risk Assessment phase: crowd modelling and business analytics for extracting knowledge from past events.
- Section 5 introduces the possible approaches to dynamic risk assessment providing some examples of where they have been used to deal with security issues.
- The threats faced by mass gathering events and the phases of risk assessment with their peculiarities are analysed in Section 6.
- Section 7 briefly analyses the weak signals sensed with the technologies developed in WP5 of LETSCROWD and provides some hints on how to use them in Dynamic Risk Assessment.
- Finally, Section 8 offers a view on how to develop the first version of the Dynamic Risk Assessment methodology that will be the core of WP3.

### 1.4 DEFINITIONS

Table 1 proposes a list of definitions that will be used across the entire document to clarify the meaning of the main concept introduced by the proposed approach.

Table 1 - Definitions

Term	Definition
Dynamic Risk Assessment (DRA)	<p>The Dynamic Risk Assessment is defined by the Health Protection Agency (HPA)<sup>1</sup> in UK as the <i>“continuous assessment of risk in the rapidly changing circumstances of an operational incident, in order to implement the control measures necessary to ensure an acceptable level of safety”</i>.</p> <p>In LETSCROWD the <b>Dynamic Risk Assessment</b> definition can be modified as follows: <i>“The continuous assessment of risk in the rapidly changing circumstances of mass gathering events, in order to implement the control measures necessary to ensure an acceptable level of safety and/or security”</i>.</p>
Hazard	Something that is dangerous and likely to cause damage
Mass Gathering	A Mass Gathering event can be defined (World Health Organisation (WHO), 2008) as: <i>“more than a specified number of persons (which may be as few as 1000 persons although much of the available literature describes gatherings exceeding 25000 persons) at a specific location for a specific purpose (a social function, large public event or sports competition) for a defined period of time. In the context of this document, an organised or unplanned event can be classified as a mass gathering if the number of people attending is sufficient to strain the planning and response resources of the community, state or nation hosting the event”</i> .
Security	Security is defined in the Cambridge Dictionary (Cambridge University Press, s.d.) as <i>“Protection of a person, building, organization, or country against threats such as crime or attacks by foreign countries”</i>
Situational Awareness	According to (Endsley M.R., 1995) <i>“Situational awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and a projection of their status in the near future”</i> .
Threat	An expression of intention to inflict evil, injury, or damage
Weak Signal	A weak signal can be defined (Paul J.H. Schoemaker, 2009) as <i>“A seemingly random or disconnected piece of information that at first appears to be background noise but can be recognized as part of a significant pattern by viewing it through a different frame or connecting it with other pieces of information”</i> .

<sup>1</sup> <http://www.istr.org.uk/docs/dynamicriskassessment.pdf>

## 2 INTRODUCTION TO RISK ASSESSMENT

### 2.1 INTRODUCTION

The proposed methodology is based on a standard risk assessment approach compliant with the following standards

- ISO 31000 “Risk management” (International Organization for Standardization, 2009);
- ISO 31010 “Risk management – Risk assessment techniques” (International Organization for Standardization, 2009).

It will then focus on the aspects arising from the specificities of addressing the mass gatherings event risk assessment and in particular:

- How to improve the current Static Risk Assessment (SRA) approaches of Law Enforcement Agencies (LEAs) using crowd modelling and analytics on past events.
- How to introduce the concept of Dynamic Risk Assessment (DRA) into the LEAs’ current practices.

The risk management process proposed by the ISO 31000/31010 International Standards and the steps in which LETSCROWD augments the standard approaches are indicated in Figure 2-1 where green boxes are the steps affected by specific LETSCROWD aspects.

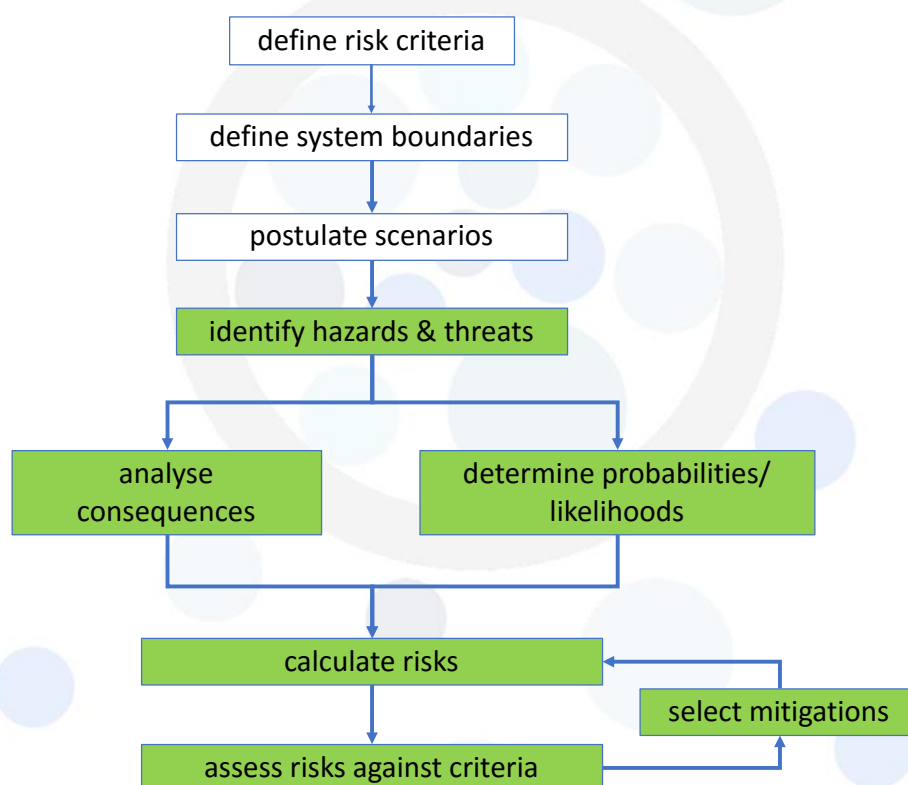


Figure 2-1 - The standard ISO 31000 procedure and LETSCROWD aspects

### 2.2 GENERAL RISK ASSESSMENT PROCEDURES

Risk assessment is a process that allows to understand risks, defining acceptable levels of risk, risk criteria and reducing risks by proposing risk mitigation.

In LETSCROWD the assessment will be limited to risk assessment for public mass gathering events only.

A risk is defined as the product of probability of hazard/threat occurrence and the severity of the resulting consequences (International Organization for Standardization, 2009):

$$\text{Risk} = (\text{Probability of hazard/threat}) * (\text{Consequences})$$

Following the ISO 31000/31010 standard, the overall procedure for risk assessment is summarised in the following paragraphs.

### 2.2.1 System boundaries definition

The **System boundaries definition** phase is essential to define precisely the physical and operational boundaries under the assessment of the mass gathering events and will involve the overall area of the event inside the main cordon as well as outside areas designated as part of the event control. The whole administration and control processes of the event is part of the system definition.

### 2.2.2 Risk criteria definition

This step is dedicated to identifying the criteria that will be used to judge the tolerability of the risks predicted during the assessment (e.g. ALARP As Low As Reasonably Possible, ALARA As Low As Reasonably Achievable, etc.). There are several options that must be considered, mainly, general principle of risk control, the risk envelope, average or peak risk, measure of risk, and values of risk limits.

Risk criteria define the frame of reference used to evaluate the significance or importance of an event's risks. The risk criteria help to determine whether an evaluated level of risk is acceptable or tolerable.

Risk criteria should reflect society's and organisation's values, policies, and objectives. They should consider the views of all the stakeholders, and should be derived from standards, laws, policies, and other requirements. The criteria will encompass the organisation operation and type of risks. These can be classified (International Organization for Standardization, 2009) as:

- human health and safety where criteria for societal risk are well established;
- operational/business;
- environmental protection;
- legal and regulatory compliance;
- cost;
- project schedule;
- reputation;
- finances.

LETSCROWD will mostly concentrate on the human health and safety risks, i.e. the health and safety of the crowd taking part to the event, the LEAs' agents and the organiser's stewards.

### 2.2.3 Postulate scenarios

In this phase, events leading to a possible risk must be postulated. A number of such scenarios associated with possible threatening attacks to the crowd will be defined at the start of the assessment. So, the analyst will choose the level of detail necessary to carry out the assessment and check the consistency of this level with the purpose of the risk assessment.

Possible sources of information for this phase are:

- The past experiences (direct or through international cooperation) of the LEAs.

- Private (intelligence) or public sources like the database of past attacks like the Global Terrorism Database<sup>2</sup> (GTD) of the National Consortium for the Study of Terrorism and Responses to Terrorism in USA.

### 2.2.4 Identify Hazards/Threats

The success of a risk analysis depends on the identification of potential hazards and threats. Hazards may emanate from two categories

- **Internal Hazards** - Hazards intrinsic to the site or activity associated with the mode of operation (i.e. the crowd and the venue)
- **External Hazards and Threats** - emanating from outside the defined operational boundaries. The identified potential accident scenarios will be used in identification of hazards for subsequent risk analysis.

The hazards and threats postulation can be considered using any historical data, expert elicitation or by means of structured brain storming. The following methods can be useful for identification of hazards and threats to ensure that the list is as comprehensive as possible:

- What-If analysis to consider what threats and hazards may occur during the event and it is carried out by people with the local knowledge of the event area, together with people with knowledge of the operations and procedures.
- Use of Checklists on the basis of past events and brain storming to identify hazards and threats which may occur.
- By means of HAZOP studies (Hazard and operability study) to identify threats and hazards. For this type of analysis, an inter-disciplinary team of experts will be required.
- Other techniques which can be used are Failure Mode and Effect Analysis (FMEA) or Fault Tree Analysis (FTA).

Once hazards and threats are identified, strategies to respond to/mitigate such hazards and threats are developed to protect the public and/or infrastructures involved. A hazard/threat log book is maintained together with groups of similar threatening events, such that if during the actual event, a threatening event occurs which has not been identified earlier, the organiser may use interpretation between analysed threats to apply a mitigation procedure which is appropriate for current threatening event. Possible options for hazard/threat control are:

- |                       |                                 |
|-----------------------|---------------------------------|
| • Elimination         | • Adequate supervision          |
| • Substitution        | • Training                      |
| • Enclosure           | • Information                   |
| • Guarding            | • Personal protective equipment |
| • Safe/secure systems | • Awareness                     |
| • Written procedures  | • Intelligence                  |

However not all these controls can be applied to all situations.

Moreover, in responding to any risk, any mitigations considered must be proportionate to benefit, so in most cases Cost Benefit Analysis (CBA) should be initiated. This is particularly important when applied to the emergency services, because individuals may be risking their personal safety to rescue others.

---

<sup>2</sup> <http://www.start.umd.edu/gtd/>



## 2.2.5 Assess probabilities/likelihood

To assess the probabilities of initial hazardous events, an analysis of historical data applicable to the given situation should be carried out, or in a case of very limited data, formalised techniques of elicitation of experts' judgement could be applied. Alternatively, a fault tree analysis (using component and human reliability data), when a combination of failure events is required, may be applied.

Likelihood of a hazard identified occurring is a function of probability of the resulting consequences being materialised, and the possibility of the subject being exposed at a given location and time. An example of a likelihood scale is given in Table 2.

**Table 2 - Example of a likelihood scale**

Scale of Likelihood		Likelihood of occurrence
Highly probable/Likely	10	It is expected to/will probably occur in most circumstances
Medium/Possible	5	It will probably occur in most circumstances
Low/Remote	2	It will/could occur some of the time
Negligible/Unlikely	1	It could occur under exceptional circumstances

## 2.2.6 Assess consequences

The consequence of the postulated accidents will be assessed considering the transient behaviour of the processes involved. The consequences leading to individual fatalities and different degree of injuries will be considered.

The consequences as a result of a hazardous event can be different depending on the organiser and/or type of mass gathering events. The consequences from any threat can be estimated using, for example, the scale presented in Table 3 (World Health Organisation (WHO), 2015).

**Table 3 – Consequence table for the crowd**

Level		Consequence on crowd
High/Severe	10	Substantial loss of life and serious injuries or illness. Widespread disruption of local services and infrastructure.
Medium/Major	5	Many deaths, injuries or illness. Disrupts public health and medical services.
Low/Moderate	2	Death and or injuries or illness occur. Public and medical services are strained.
Minor	1	Few illness or injuries which public health and medical services can manage.

The consequence scale shown above could be adapted for different types of consequences including safety, business, environment, the event organiser, etc.: an example in Table 4 (World Health Organisation (WHO), 2015).

**Table 4 – Consequence table for the organiser and the mass gathering**

Level		Consequence on crowd
High/Severe	10	Event causes cancellation of some or all of mass gatherings. Significant adverse impact on mass gatherings and host reputation.
Medium/Major	5	Event is disruptive to mass gatherings and reputation of host
Low/Moderate	2	Some controlled impact on the mass gathering and reputation for host



Minor	1	Small impact on mass gathering, can be managed with little impact on the event
-------	---	--

### 2.2.7 Assess Risk

For each potential hazard considered, the level of risk will be evaluated from the level of consequence and the probability of the hazard occurring.

After having set the values obtained for likelihood and consequence for a given threat, asset and risk type, a risk level is estimated using a risk matrix as shown in Table 5 below (cells in red correspond to HIGH risk, yellow to MEDIUM risk and green to LOW risk).

**Table 5 - Example of a risk matrix (for each type of risk)**

Likelihood of threat(s)	Highly probable/Likely	10	20	50	100
	Medium/Possible	5	10	25	50
	Low/Remote	2	4	10	20
	Negligible/Unlikely	1	2	5	10
	Minor	Low/Moderate	Medium/Major	High/Severe	
	Consequences (severity) of associated threat(s)				

The risk can fall into:

- Low Risk (green) – can be considered as acceptable without review,
- Medium Risk (yellow) – Acceptable risk level but review is required by management and controls put in place,
- High Risk (red) – Risk reduction is required to acceptable level.

The identified risks should be recorded in a risk log for future assessment and monitor how these could vary as function of time.

### 2.2.8 Assess risk against criteria

Once the risk level is evaluated it will be assessed against defined risk criteria. For events exceeding the criteria, measures must be postulated for reduction of this risk to an acceptable level.

### 2.2.9 Risk reduction/mitigation measures and related procedures

For events exceeding the risk criteria, measures must be identified for risk reduction /mitigation. In this process it is necessary to ensure that ALARP (As Low As Reasonable Practicable) is demonstrated. The mitigation could be based on methods for reduction in the level of consequence or reduction in frequency of the hazard (Federal Emergency Management Agency (FEMA), 2005). In most cases procedures for how to deal with such risks must be written and checked for practicality. In all cases training in safety and risk should be initiated for all involved in safety management. Especially, the written procedure could be very useful for controlling dynamic risks.

More details on the risk reduction/mitigation measure will be considered in LETSCROWD Task 3.3 and related deliverables.

The mitigation procedures should be documented to present the mitigation strategy. Once reviewed and submitted to relevant stakeholders and responsible people, these should be adopted. These procedures

should be also checked and updated with time to ensure applicability at a given time, e.g. procedure to be taken receipt of bomb threat<sup>3</sup>.



---

3

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/552301/Bomb\\_Threats\\_Form\\_5474.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/552301/Bomb_Threats_Form_5474.pdf)

### 3 DYNAMIC RISK ASSESSMENT (DRA) REQUIREMENTS

This section summarises the requirements for the Dynamic Risk Assessment extracted from:

- The European Security Model (ESM);
- The activities carried out in WP2 and reported in Deliverable D2.2;
- The feedback received from the LEAs involved in the project.

#### 3.1 THE EUROPEAN SECURITY MODEL (ESM)

The Internal Security Strategy for the European Union (Council of the European Union, 2010) has defined a European Security Model (ESM). The ESM consists of *“common tools and a commitment to: a mutually reinforced relationship between security, freedom and privacy; cooperation and solidarity between Member States; involvement of all the EU's institutions; addressing the causes of insecurity, not just the effects; enhancing prevention and anticipation; involvement, as far as they are concerned, of all sectors which have a role to play in protection – political, economic and social; and a greater interdependence between internal and external security”*.

In particular, the ESM prescribes the following:

- *“... stronger focus on the **prevention of criminal acts** and terrorist attacks before they take place can help reduce the consequent human or psychological damage, which is often irreparable. Our strategy must therefore emphasise **prevention and anticipation**, which is based on a proactive and intelligence-led approach ... Furthermore, it is necessary to develop and improve prevention mechanisms such as analytical tools or early-warning systems.”*
- *“This allows us to deepen our **understanding of the different types of threats and their probability** and to anticipate what might happen ...”*
- *“**Guidelines for hazard and risk-mapping methods, assessments and analyses** should be developed as well as an overview of the natural and man-made risks that the EU may face in the future.”*

#### 3.2 REQUIREMENTS FROM DELIVERABLE D2.2

The following are the requirements on Dynamic Risk Assessment (DRA) extracted from the LETSCROWD Deliverable D2.2:

- |        |   |
|--------|---|
| DRA_01 | The tool shall provide security practitioners with an extension of the European Security Model (ESM) implementation guidelines tailored to the needs of crowd protection during mass gatherings |
| DRA_02 | The tool shall allow a Static Risk Assessment (SRA) and a Dynamic Risk Assessment (DRA)   |
| DRA_03 | The tool shall allow a Static Risk Assessment (SRA) based on the current practices of involved LEAs possibly augmented with the WP5 technologies  |
| DRA_04 | The tool shall allow a Dynamic Risk Assessment (DRA) based on the fusion of heterogeneous weak signals  |
| DRA_05 | The tool shall address security events only   |
| DRA_06 | The tool shall allow to assess consequences and related mitigations on the basis of the modified risk conditions from DRA using both the dynamic crowd model and the Real-time Evacuation tool  |
| DRA_07 | During DRA, the tool shall allow to properly manage the uncertainty linked to the fusion of the heterogeneous weak signal involved in the process to take risk-aware decisions                  |

- DRA\_08 The strategic long-term decisions part of DRA shall be based on post-event forensic analysis of the dynamic evolution of the risk conditions: changes to the current mitigations solutions, improved communications solutions, training of the staff, etc.
- DRA\_09 The tool will be first in English, and then translated into other languages after it is proved to be reliable
- DRA\_10 During DRA the tool shall be able to detect patterns of weak signals representing a specific threat and its associated likelihood and possible consequences
- DRA\_11 The weak signals to be used by DRA should come from heterogeneous sources including crowd as sensor, security personnel as sensor, video analysis from cameras on poles, video analysis from cameras on drones, social media analysis, etc.
- DRA\_12 When dealing with weak signals, the DRA tool shall consider also the environmental conditions that transform an apparently insignificant signal into threats
- DRA\_13 The DRA tool shall allow to define risk criteria and system boundaries, postulate scenarios and identify threats (according to ISO 31000).
- DRA\_14 The DRA tool shall allow to list and display weak signals with trustable geo-localisation information and time stamp
- DRA\_15 The DRA tool shall graphically display geographic and/or time correlations between weak signals.
- DRA\_16 The DRA tool shall attract operators' attention on weak signals and/or patterns of weak signals that could become threats and also alert operators when these become threats highlighting them using alert scales.
- DRA\_17 The DRA tool shall include a juridical recorder to allow forensic analysis by securely storing all the received weak signals, the detected patterns of weak signals and the sequence of decisions taken by the operator
- DRA\_18 The IT infrastructure supporting the collection of weak signals and its delivery to DRA tool shall ensure a correct time sequence by using a universal trustable time source.
- DRA\_19 Records and documentation as part of the police and judicial proceedings

### 3.3 FEEDBACK FROM VISIT TO LAW ENFORCEMENT AGENCIES (LEAS)

#### 3.3.1 Introduction

The feedback from LEAs has been collected:

- At the plenary meetings of the Consortium.
- During a visit to the following LEAs:
  - Local Police Voorkempen (LPV, Belgium) on 24 October 2017 in Antwerp.
  - Ayuntamiento de Madrid (ADM, Spain), Gobierno Vasco Departamento Seguridad (ERT, Spain) and Ministerio Da Administracao Interna (PSP, Portugal) on 8 November 2017 in Valencia at ETRA premises.
  - Hochschule Fur Den Offentlichen Dienst in Bayern (BayFHVR, Germany) on 9 November 2017 in Munich.

#### 3.3.2 Synthesis of the visits to LEAs

The feedback from the LEAs can be summarised in the following points:

- All LEAs are carrying out Static Risk Assessment for mass gathering events using similar qualitative approaches based on national regulations and having as a basis the ISO 31000 standard (International Organization for Standardization, 2009). An example is the "Veranstaltungssicherheit" Manual used by BayFHVR.
- The risk assessment for mass gathering events is organised in strict cooperation with the event's organiser (a private or public organisation that normally starts the procedure). Normally, the organiser assesses the safety risks while the LEAs are reviewing and, if needed, revising the safety assessment implemented by the organiser adding the security risks. An example of the organisation of a security event is given in Section 10 "Appendix 1 - Example of a security event in Germany".
- The level of risk (in a scale of 3 or 5 levels) for all possible threats is typically determined by the commander assigned to the event according to his experience (or more in general expert knowledge) and the collected information.
- Currently LEAs do not use any specific SW tool, using mostly brainstorming to statically and dynamically assess the risks of an event.
- The level of risk is typically assessed locally (municipality/province) and escalated at the national level only if necessary.
- Local regulations are affecting the way in which risk is assessed in each regional or national territory. An example is the New Bavarian law to be published in early/mid 2018 which will regulate the CCTV crowd surveillance and will therefore have an impact on LETSCROWD suspicious behaviour and suspicious objects detection.
- Data related to past events is collected, even if not always systematically, but, at least at the local level, automated analytic tools are not yet used to elicit knowledge from data.
- Man must be "in-the-loop" in any decision step. Automated tool can only be in support to the decision-making process and final decision shall be left to responsible person(s).
- Each sensed weak signal should include
  - Time
  - Geolocation (if available/feasible)
  - Type of weak signal
  - Snapshot and/or synthetic information related to the event it is referring to
  - Possibly reliability of the information
- The DRA approach should be focused mostly on prevention activities.

These aspects will be incorporated into LETSCROWD methodology.

## 4 IMPROVEMENTS TO STATIC RISK ASSESSMENT

Currently in Europe mass gathering events are already supported by well-defined **Static Risk Assessment** procedures based on traditional static information gathering approaches to determine possible safety and security risks and related mitigations. This has been confirmed by the interviews to the LEAs involved in LETSCROWD.

Moreover, according to the feedback from LEAs (Section 3.3), the current Static Risk Assessment approaches could be improved with the introduction of:

- Crowd modelling and simulation tools to better analyse possible consequences on crowds during evacuation in the presence of a given attack.
- Analytics tools to better process past data archives to find correlations and compute risk parameters (e.g. the likelihood of a given event). These approaches have been recently introduced and heavily rely on the performances of the technology and on the availability of (well structured) data.

The above aspects are described in more detail in the following sections.

### 4.1 CROWD MODELLING

Crowd modelling for mass gatherings is an assessment of the likely dynamics, behaviour and characteristics of a crowd, most commonly undertaken during the planning of the mass gathering. Currently, the assessment is most commonly undertaken by expert consultants on behalf of event organisers or LEAs to assess the following:

- What is the capacity of different areas of the Mass Gathering? (e.g. viewing areas, routes, entry points)
- Forecast various characteristics of the crowd related to safety (e.g. density, speed, evacuation time) during different scenarios (ingress, circulation, egress, emergency)
- Test “what if” scenarios for crowd movement, including emergency egress situations

An important element of crowd modelling is the simulation of crowds using advanced computer algorithms. This type of software can provide a detailed analysis of the effects on a crowd during a mass gathering. Task 5.1 aims to develop such a tool that can be used by experts in crowd modelling (possibly required of the event organiser) or even LEAs themselves, albeit by a trained operator.

This type of analysis and the Task 5.1 simulation can be used throughout the SRA process for one or more of the following purposes as appropriate to the mass gathering and risks being assessed:

- Identify potential hazards to crowd safety by testing different scenarios (e.g. during egress, the simulation identifies high crowd density at one exit)
- Measure potential consequences of identified hazards to the crowd. For example:
  - Potential Hazard: a route may have to be closed due to nearby construction
  - Crowd Modelling: The simulation will test the impact this may have on the crowd movement
  - Consequence: the simulation results show low density when crowds reroute, meaning consequence can be considered low
- Plan for and optimise proposed mitigation procedures, relating to crowd management, that arise from SRA
- Re-test consequences after risk mitigation has been identified

Such results could help the quality of risk assessment, and identify new risks based on crowd movement or proposed LEA tactics.



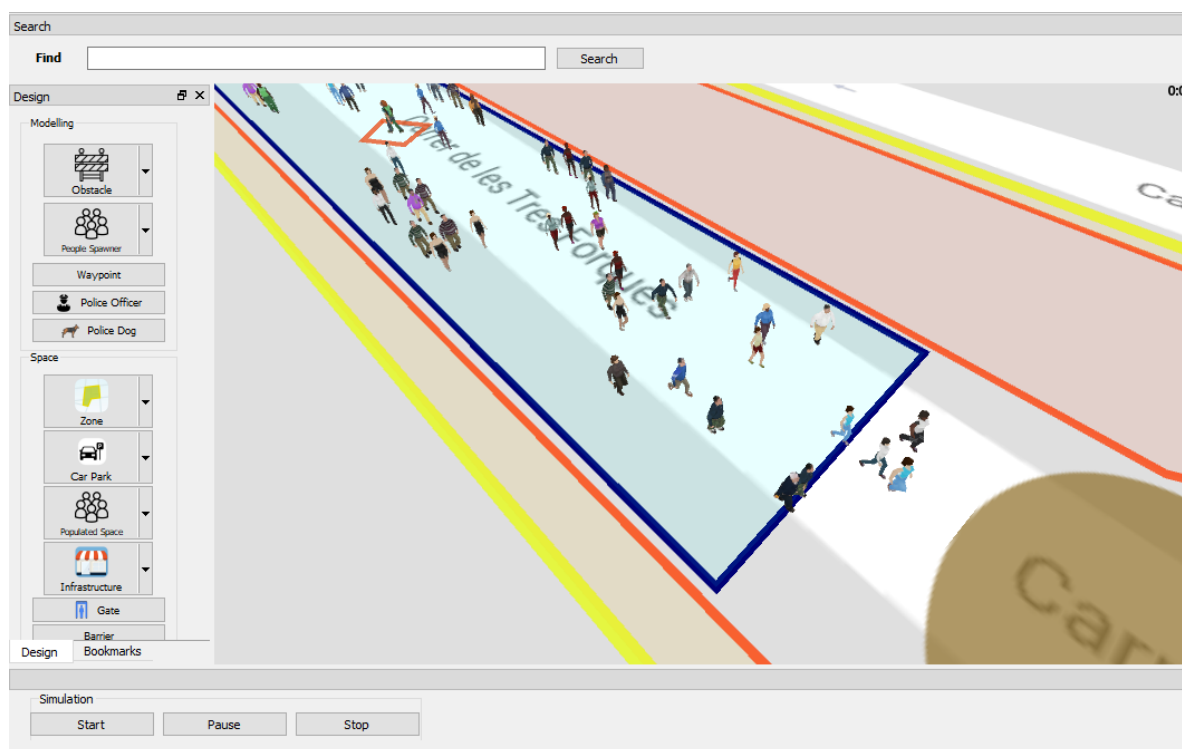


Figure 4-1 - Example of crowd simulation from T5.1

## 4.2 ANALYTICS ON EXISTING DATABASES

The use of big data analytics for criminal and forensic investigation is starting to be a hot topic in both the academia and law enforcement agencies daily use (e.g. the Detroit Crime Commission<sup>4</sup> is using data analytics tools to find human and crime relationships<sup>5</sup>).

According to (Pramanik M.I., 2017), analytics on criminal data can be applied for:

- **Relational Analysis Purposes:** to extract patterns of criminal activities, to predict the probable time and place of crime to take place, and to identify the different members of a criminal network through behavioural profiling.
- **Positional Analysis Purposes:** to answer questions like “What types of roles does a specific individual or group appear to be playing within a criminal network?”.

More work on this topic is expected to be carried out in LETSCROWD WP4.

<sup>4</sup> <https://detroitcrimecommission.org>

<sup>5</sup> [https://www.datameer.com/wp-content/uploads/2015/09/detroit\\_crime\\_commission\\_testimonial.pdf](https://www.datameer.com/wp-content/uploads/2015/09/detroit_crime_commission_testimonial.pdf)



## 5 POSSIBLE APPROACHES TO DYNAMIC RISK ASSESSMENT

The risk assessment can be conducted using a) qualitative or b) quantitative risk assessment methods as extensively described in (Haimes, 1988) and (Vose, 2000).

**Qualitative risk assessment:** The qualitative risk assessment approach is based on identifying threats/hazards and consequences and evaluating the estimated risks from the perceived likelihood and consequence of each. For example, scales such as those shown in Table 2, Table 3 and Table 4 below can be devised to categorise the likelihood and consequence of a given risk event.

The evaluated risk can then be categorised (e.g. as “low”, “medium” or “high”) using the “Boston Square” method (International Organization for Standardization, 2009). The Boston Square approach has the advantage of relative simplicity but is very subjective and open to bias.

**Quantitative risk assessment:** Quantitative techniques may be more appropriate in several circumstances, including:

- when there are concerns that significant hazards/threats may be overlooked by qualitative approaches;
- where there may be uncertainties over the likelihood or consequence (or both) of a system going wrong and where quantifying these may reduce uncertainty;
- where qualitative assessments indicate a significant number of high risks in a system, hence there is a need to prioritise risk reduction or mitigation work using more robust techniques, especially when significant levels of spending are required.

The quantitative risk analysis techniques available are generally those that have been used in health and safety and natural disaster risk assessment for some time. However, it is important to understand some of the limitations of these techniques when applied to mass gathering event risk assessment. These are discussed in some detail in the following section.

The more detailed risk assessments may be based upon a scenario approach or be based upon Monte Carlo simulation (probabilistic systems assessment (PSA) approach) taking advantage of qualitative data and quantitative inputs and assessments.

### 5.1 QUALITATIVE APPROACHES

The simple qualitative risk assessment approach is based on identifying threats/hazards and consequence and evaluating the estimated risks from the perceived likelihood and consequence of each threat/hazard. The likelihood values of a hazard can be estimated using:

- Historical data
- Elicitation from experts
- Fault tree analysis

Qualitative approaches can benefit from the adoption of GIS-based situational awareness tools to help stakeholders in:

- Having a correct understanding of time-varying scenarios;
- Immediately perceiving changes in the level of risks.

### 5.1.1 Historical data collection

The systematic collection of prior knowledge from historical data is intended to identify existing information that may help the risk assessment process, but care must be exercised to ensure data relevancy.

The consequences associated from a given hazard can be obtained from historical data or empirical evaluation or modelling. The fatalities and injuries caused by an accident can be scaled up or down on the basis of the size of the event and on the changing habits of event organisers. Using modelling software e.g. HAZUS<sup>6</sup>, it is possible to estimate number of fatalities and injuries resulting from different strength earthquakes, floods and strong winds: similar approaches could be adopted also for the mass gathering security issues faced by LETSCROWD. As an example, the consequence of a bomb blast on evacuation distance can be estimated by and using the data provided by Office of the Director of National Intelligence<sup>7</sup> shown in Figure 5-1.









Bomb Threat Stand-Off Distances				
Threat Description		Explosives Capacity <sup>1</sup> (TNT Equivalent)	Building Evacuation Distance <sup>2</sup>	Outdoor Evacuation Distance <sup>3</sup>
	Pipe Bomb	5 LBS/ 2.3 KG	70 FT/ 21 M	850 FT/ 259 M
	Briefcase/ Suitcase Bomb	50 LBS/ 23 KG	150 FT/ 46 M	1,850 FT/ 564 M
	Compact Sedan	500 LBS/ 227 KG	320 FT/ 98 M	1,500 FT/ 457 M
	Sedan	1,000 LBS/ 454 KG	400 FT/ 122 M	1,750 FT/ 533 M
	Passenger/ Cargo Van	4,000 LBS/ 1,814 KG	600 FT/ 183 M	2,750 FT/ 838 M
	Small Moving Van/ Delivery Truck	10,000 LBS/ 4,536 KG	860 FT/ 262 M	3,750 FT/ 1,143 M
	Moving Van/ Water Truck	30,000 LBS/ 13,608 KG	1,240 FT/ 378 M	6,500 FT/ 1,981 M
	Semi-Trailer	60,000 LBS/ 27,216 KG	1,500 FT/ 457 M	7,000 FT/ 2,134 M

Figure 5-1 - Explosive evacuation distance

### 5.1.2 Elicitation of knowledge from experts

The data for risk evaluation, outlined above, can be elicited from experts. It is suggested that this data collection will include:

<sup>6</sup> <https://www.fema.gov/hazus-software>

<sup>7</sup> [https://www.dni.gov/files/NCTC/documents/features\\_documents/2006\\_calendar\\_bomb\\_stand\\_chart.pdf](https://www.dni.gov/files/NCTC/documents/features_documents/2006_calendar_bomb_stand_chart.pdf)

- 1) Hazards and threats applicable to crowd gathering and management,
- 2) Likelihood of occurrence (according to and agreed scale),
- 3) Consequences' magnitude (according to and agreed scale),

The elicitation can be conducted with individual experts separately or by means of group elicitation.

The advantage of a group session is that the interactions between participants with differing experience and expertise tend to promote broader thinking and take better account of the interfaces between subsystems and activities. Such sessions can also have more immediate and wider benefits in terms of the overall safety culture, by promoting awareness of existing hazards and understanding of differing viewpoints.

In the formal group elicitation, the format of such sessions is usually based on the application of a set of prompts (keywords) to some structured breakdown of the system or process being considered. Thus, for example, keywords such as NOT DONE or MISUNDERSTOOD can be applied to each task in a procedure to prompt participants' thinking about how it might go wrong. The structured format promotes comprehensive consideration of the problem, whilst the keywords encourage creative thinking.

The elicitation from experts can concentrate on individual value, or on parameter distribution representing uncertainty. The evaluated risk can then be categorised as "low", "medium" or "high" using the "Boston Square" method described earlier.

Assessing the risk against risk criteria, any risk above the criteria must be reduced, by decreasing the likelihood or decreasing the consequence. This process of risk reduction is mitigation process.

The uncertainty treatment in the case of a lack of a mathematical model, is to elicit the risk values by asking the experts to provide the values by means of 'subjective' Probability Density Function (PDF) reflecting the expert belief regarding the value range. The experts can also judge the shape of the PDF. The experts can select the PDF from a range of functions (e.g. see Table 6).

In practice Uniform PDF is quite useful where only minimum and maximum values are available. A Triangular distribution function is also very useful, since it can be defined by three parameters: minimum, most likely and maximum values, and has the advantage that it is easy to visualise and understand their mining.

**Table 6 - Example of Probability Density Functions (PDF)**

PDF	Representative values	PDF	Representative values
Uniform	Min, Max	Normal	Mean, Standard Deviation (SD)
Triangular	Min, Max, Mode	Exponential	Min, Mean
Beta	Min, Max, Mean, SD	Gamma	Min > 0, quantile

Expert elicitation sessions should be prepared and conducted in such a way so as to reduce the bias in subjective judgement and errors in the result outcome. The participants in the elicitation exercise should be provided with a briefing document outlining the elicitation procedure and it should be stressed that consensus is not the main goal of the process. The elicitation of risk value should follow the methodology outlined in previous chapter. The risk value from each expert can be a single value or PDF parameters depending on the type of risk considered. The elicitation session is normally followed by post-elicitation discussion and feedback analysis of outcome and aggregate of results.

### 5.1.3 Fault Tree Analysis

Fault Tree Analysis (FTA) is a systematic method of system analysis that examines the system using a top-down approach providing graphical symbols for easy of understanding and incorporates mathematical tools to focus on critical areas. Logic trees are important tools for exploring the scenario space, analyzing uncertain events, defining scenarios, and assessing risks. According to ISO31010 (International Organization for

Standardization, 2009), FTA is a “*technique which starts with the undesired event (top event) and determines all the ways in which it could occur. These are displayed graphically in a logical tree diagram. Once the fault tree has been developed, consideration should be given to ways of reducing or eliminating potential causes / sources*”. FTA can provide both qualitative and quantitative outputs and can be used for risk identification and analysis.

FTA has started to be used also to analyse terrorism risk both qualitatively to assess bioterrorist risks to the U.S. food supply (Hope, 2004) and quantitatively to assess terrorism risk in U.S. (Ezell B.C., 2010).

#### 5.1.4 Situational awareness and Geographic Information Systems

Another tool for planning and monitoring a public event is time dependent Geographic Information Systems (GIS). A GIS is a sophisticated mapping application which is built on the concept of spatial data.

The system allows to visualise site information, demographic and any other data with a spatial component. A major concept of GIS is ease of viewing such data, and in particular time dependent data.

For the application to public events, the venue area is represented as a map of the area large enough to show all the cordons setup by the organisers with the help of the relevant services, police, fire brigade, emergency services. The map of all local streets and major buildings could be mapped in this way together with any useful information.

Other data which could be useful is as follows:

- All ingress/egress locations to the venue (time dependent),
- Amenities on the event site,
- Position of emergency services, rescue centres,
- Risk areas,
- Procedures for emergency, (risk), bomb location and disposal,
- Evacuation routes,
- Location of unattended packages (as the information is coming)

GIS can also be used to:

- Control and or simulate the movement of public in emergency,
- Display CCTV video streams as they are received,
- Display ad geo-locate alerts (see Section 5.1.5 for a more detailed discussion)
- Track movement of suspected terrorists/lone wolves as function of time,
- Quickly recover useful information for the management of emergency
- Other information.

Current COTS real-time GIS products (e.g. ArcGIS from ESRI<sup>8</sup>) are typically able to answer questions like:

- Where are additional Urban Search and Rescue teams necessary to improve response time and capability?
- Where should fire stations be located if a five-minute response time is expected?

<sup>8</sup> <http://www.arcgis.com/features/index.html>

- How many paramedic units or ambulances are required, and where should they be located?
- What are alternative routes?
- What facilities will provide evacuation shelters?
- What quantity of supplies, bed space, and so forth, will be required at each shelter based on the number of expected evacuees?

Therefore, GIS tool could be a very useful tool for planning the event, monitoring and control of large events.

Within the LETSCROWD project, Task 5.1 is developing crowd simulation based on GIS. This will allow geo-located data to be displayed or input. For example, a location where a hazard is identified, reported incidents, identified location of a terrorist or other person/object by time. This could be used in combination with existing COTS GIS products to further aid the assessment of risk.

GIS could also be a very useful tool for planning the event, monitoring and control of large events, and as a dynamic risk assessment progresses, for example by recording and displaying the location of weak signals arriving from various sources or input manually by the user. Some screen shots of the potential for this system used to place risk are shown in Figure 5-2 (geo-location of risk, use of cordons (e.g. bomb explosion radii), management positions can be recorded) and Figure 5-3 (input new hazard and calculate level of risk that is geo-located).

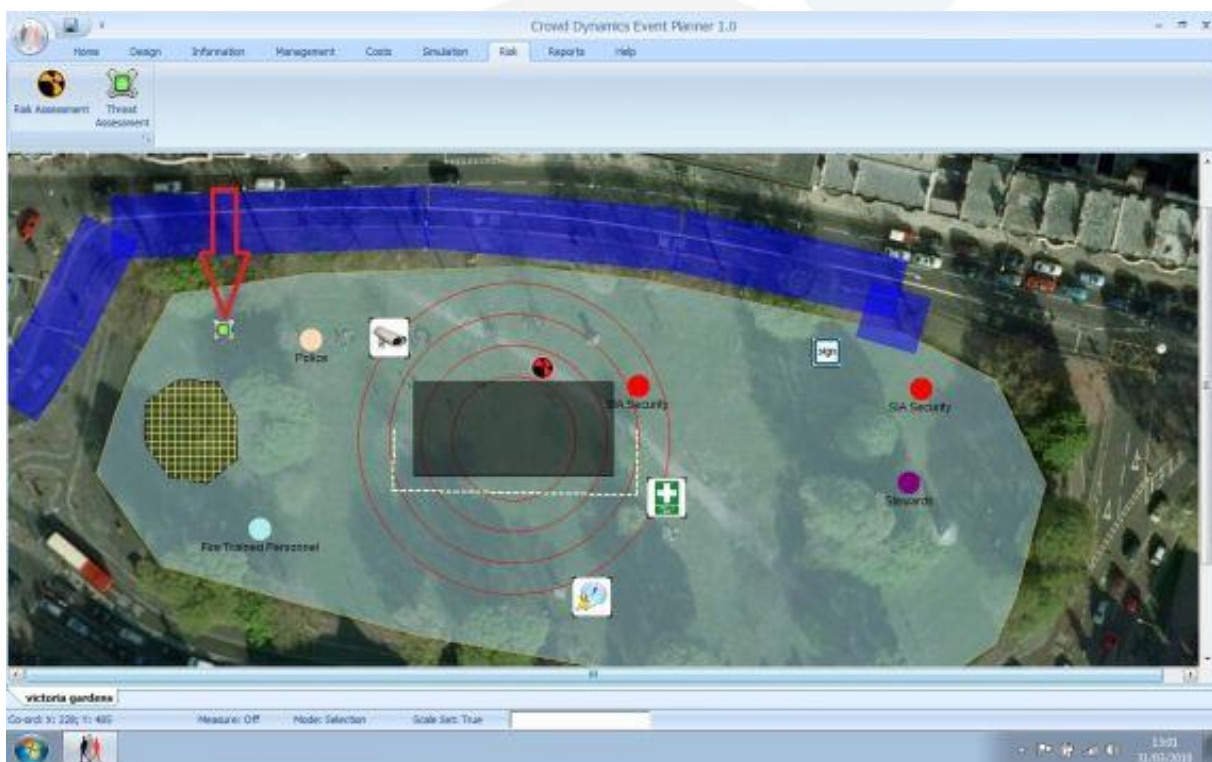


Figure 5-2 – Possible use of GIS-based tools (1)



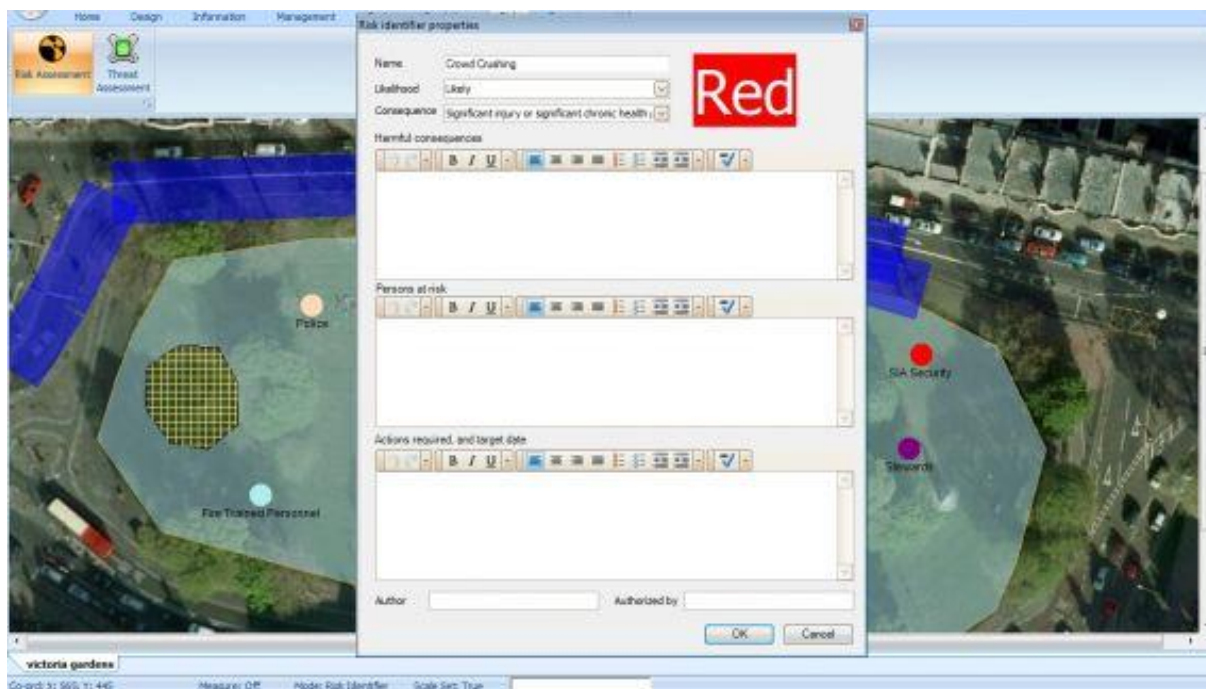


Figure 5-3 – Possible use of GIS-based tools (2)

## 5.1.5 Georeferenced time-stamped alerts

### 5.1.5.1 Alert representation

The adoption of situational awareness tools involves the correct representation of an alert (e.g. the detection of a suspicious behaviour in a given area of the mass gathering venue) in a real-time GIS. To this end, the OASIS consortium<sup>9</sup> has developed the CAP - Common Alerting Protocol (OASIS Consortium, 2010).

The Common Alerting Protocol (CAP) provides an open, non-proprietary digital message format for all types of alerts and notifications offering the following capabilities:

- Flexible geographic targeting using latitude/longitude shapes and other geospatial 9 representations in three dimensions;
- Multilingual and multi-audience messaging;
- Phased and delayed effective times and expirations;
- Enhanced message update and cancellation features;
- Template support for framing complete and effective warning messages;
- Compatible with digital signature capability; and,
- Facility for digital images and audio.

A CAP alert message consists of an <alert> segment, which may contain one or more <info> segments, each of which may include one or more <area> and/or <resource> segments where:

- The <alert> segment provides basic information about the current message.

<sup>9</sup> <https://www.oasis-open.org>

- The <info> segment describes an anticipated or actual event in terms of its urgency, severity and certainty.
- The <resource> segment provides an optional reference to additional information related to the <info> segment within which it appears in the form of a digital asset such as an image or audio file.
- The <area> segment describes a geographic area to which the <info> segment in which it appears applies.

The CAP alert message model extracted from the CAP standard is described in Figure 5-4.

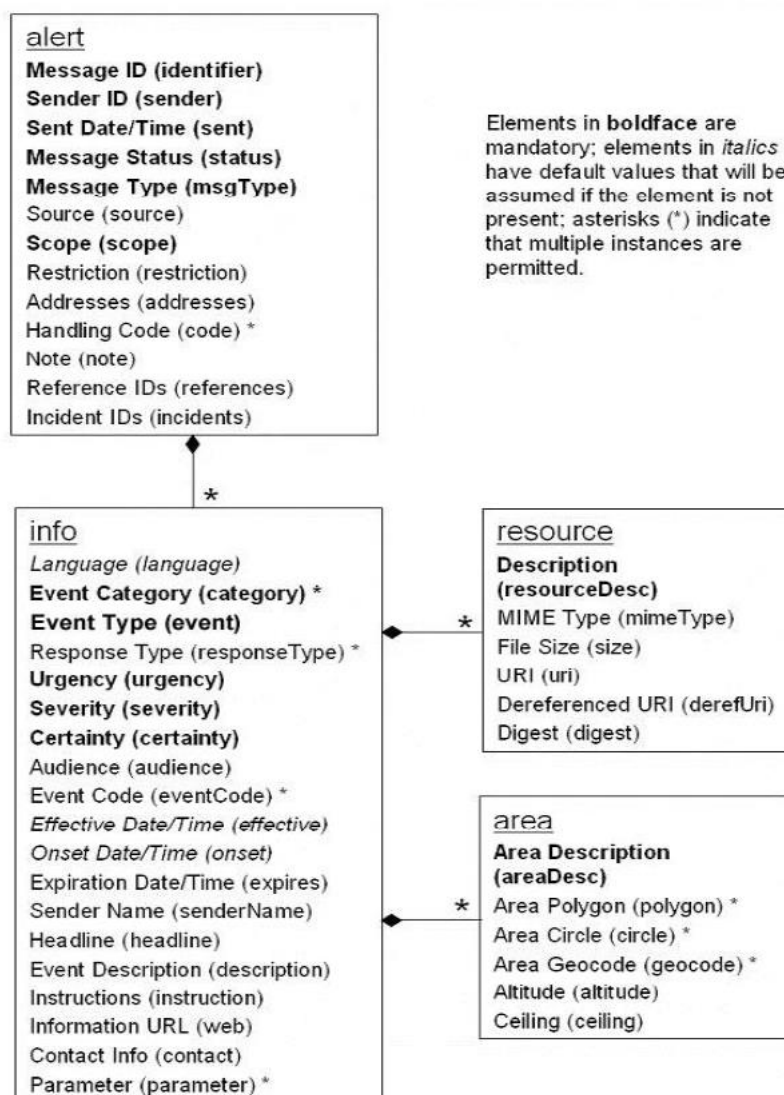


Figure 5-4 - The CAP alert message model

The CAP alert message model could be considered as the basis for the formalisation of the LETSCROWD alert message model to be used to manage situational awareness.

#### 5.1.5.2 Alert-based risk assessment

Some recent developments (Chakir E., 2017) in the network Intrusion Detection Systems (IDS) area have proposed an approach to qualify the level of dangerousness (linked to the risk) of alerts as the product of several parameters as represented by the list in Table 7.



**Table 7 - IDS parameters for alert dangerousness**

Parameter	Description
Priority (P)	This value measures the severity of an alert; it takes no account of the environment or the host to be protected.
Value of the Destination Device (D)	This is a value to define the importance of a machine on the network.
Reliability (R)	In terms of risk, this parameter could be called “Reliability”. This is defined for each independent event. The term reliability can therefore be translated by the reliability that an alarm is not a false positive.
The severity of Alert (S)	Severity level is associated with each generated alert to help us to know the threat represented by the event.

The dangerousness is then computed using the following product:

$$D(alert_i) = \frac{(P) * (D) * (R) * (S)}{normalising\ factor}$$

This, or similar, qualitative approaches could be used to assess the dangerousness – and therefore dynamically update the risks – by, for example, modifying the parameters as per

**Table 8 - Example of LETSCROWD alert dangerousness parameters**

Parameter	Description
Reliability (R)	It represents the reliability of the source that has generated the alert.
Harm (H)	Level of harm that the threat(s) associated to the alert may cause to the crowd.
Priority (P)	It represents the priority of the source that has generated the alert.
Severity (S)	Level of severity of the threat(s) associated to the alert

The dangerousness formula could be updated accordingly:

$$D(alert_i) = \frac{(R) * (H) * (P) * (S)}{normalising\ factor}$$

The obtained value can be then further processed to dynamically assess the risks.

## 5.2 QUANTITATIVE APPROACHES

Quantitative risk analysis uses mathematical modelling to represent the possible consequence outcome and risk. It also uses simulation by means of mathematical models to represent uncertainty in parameter values using probability distribution to simulate system under assessment. In general, it is a more elaborate and more costly assessment to investigate uncertainties and risks, as compared to the qualitative techniques. It allows to represent uncertainties in parameters values and processes and the likelihood of meeting desired goals and targets.

The more detailed risk assessments may be based upon a scenario approach or be based upon Monte Carlo simulation - or more generally on Probabilistic Systems Assessment (PSA) approach - representing the whole system under investigation or only the critical system processes.

### 5.2.1 Bayesian Networks (BNs)

Assuming a probabilistic Bayesian world model, there are many possible approaches to reason about risk for situational awareness. The most commonly used in literature is the approach based on Bayesian Networks (BNs). As reported in (Ben-Gal, 2007) *“Bayesian Networks (BNs) belong to the family of probabilistic graphical models (GMs). These graphical structures are used to represent knowledge about an uncertain domain. In particular, each node in the graph represents a random variable, while the edges between the nodes represent probabilistic dependencies among the corresponding random variables”*.

Some examples are reported in literature:

- The use of BNs for situation assessment in military context (Bladon P., 2002), where a suite of two sensors is used to determine if an aircraft is friend or foe.
- BNs in the military domain (Linwood D. Hudson, 2005) have been used to assist anti-terrorism planners at military installations to draw inferences about the risk of terrorist attack combining information from multiple disparate sources, most of which involve intrinsic and irreducible uncertainties.
- BNs have been proposed to predict the likelihood of a terrorist attack at critical transportation infrastructure facilities (Jha, 2009).
- BNs have been used to consider **cascade (domino) effects** into risk assessment (Nima Khakzad, 2014). A domino effect is defined as a very low-probability high-consequence major accident consisting of a chain of accidents in which a primary accident escalates and triggers other secondary or higher-order accidents. In mass gathering effects a cascade effect can be generated, for example, by a terrorist alert that, spreading through the crowd, generates panic that forces crowd to evacuate thus generating injuries and fatalities. In this case BNs are used to update probabilities of the cascade effects in which each state is represented by a BN's node.

### 5.2.2 Probabilistic Decision Trees (PDTs)

There are two main possible approaches within the PDTs family

- Best-Case/Worst Case scenarios
- Decision Trees

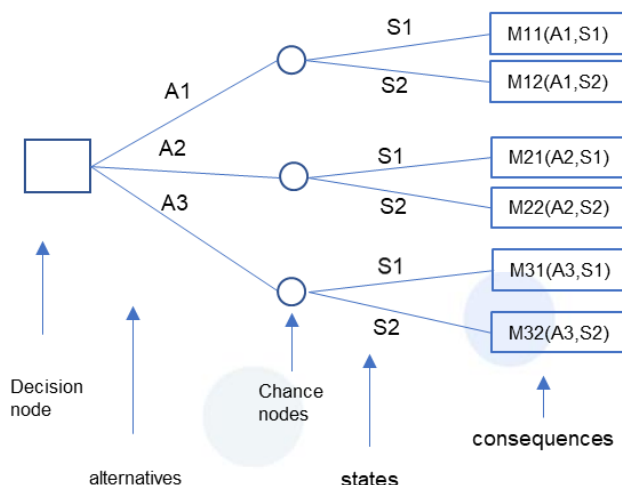
**Best-Case/Worst-Case** - The procedure here is to identify scenarios which will lead to a Best-Case outcome or worst outcome. In such situations if the Worst-Case risk scenario indicates that this will not lead to a catastrophic event and it can be managed, the assessor will not need to investigate further.

Using this approach, the decision making is most conservative and permits to identify conditions where the minimum gain is maximized or alternatively the maximum loss is minimised.

**Decision Trees** - Where risk is not only discrete but also sequential, a **Decision Tree** (Waters D., 2011) can be used to analyse risks. Methods in which risk is derived by summing up the contributions to the total risk from all significant event types. In these methods the event probabilities and outcomes are derived separately.

The start of the decision process is the root of the tree, every event is representing a possible risky option, the decision makers' choices are the decision trees' choices and the end nodes represent final outcomes.

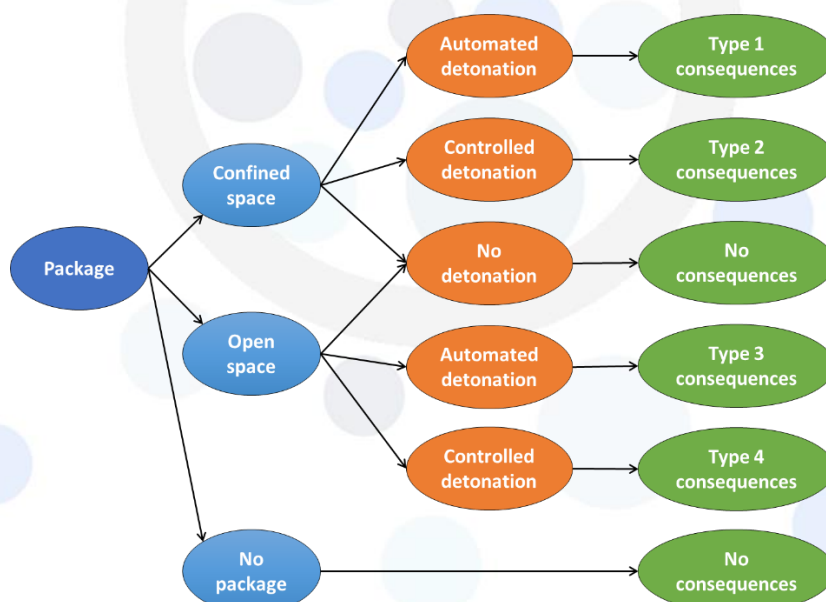
.



**Figure 5-5 - A generic decision tree**

Figure 5-5 shows a typical generic tree representing the decision node, the chance node and consequences.

Figure 5-6 below represents modelling of a left luggage in public place which is suspected of containing explosive. The options modelled is luggage in 1) an enclosed space, 2) open space, and 3) no explosive package left. For each left luggage option, the detonation may be controlled (i.e. detonated by remote control), or by means of automatic detonation (i.e. timer). The consequence will depend on the number of people affected and whether the package was left in confined or open space. (generally, explosion in confined space is more severe. The model may use discrete or continuous distribution to represent probabilities.



**Figure 5-6 - Unidentified left package in public place**

A similar approach can be undertaken with suspect car or a lorry. The main difference will be the amount of explosive that can be carried in vehicles as compared to packages.

The benefit of using decision trees are:

- Dynamic response to risk
- Generates traceable value of information
- Provides better understanding of risk management

An application of PDTs to terrorist risk analysis has been proposed in (Ezell B.C., 2010), but the conclusions are that *“significant debate remains on the underlying assumption that terrorists have the understanding to always make optimal choices that maximize consequences in the wide array of challenging technical disciplines required for successful execution of a bioterrorism attack”*.

In summary, decision trees provide a flexible and powerful tool when dealing with risk that occurs in phases.

### 5.2.3 Simulations

If scenario analysis and decision trees are techniques that help the user assess the effect of discrete risk, simulation can provide a way of assessing the consequences of continuous risk. Since real life can give rise to hundreds of possible outcomes, a simulation will provide a more complete picture of the risk.

#### 5.2.4 Monte Carlo simulations

Monte Carlo sampling simulations are methods in which risk is derived directly from a “complete” representation of the system under all possible conditions. In these methods, the probability of any particular event and any associated uncertainty is implicitly accounted for in the distributions of possible values assigned to its inputs.

Typically, the proper treatment of uncertainty will involve:

- Characterising the full range of system behaviour in a conceptual model, or models, of the system;
- Establishing the parameters which influence system behaviour and their ranges of possible values;
- Investigating the behaviour of the system over the range of inputs;
- Testing the results of the investigation for completeness;
- Analysis of the results to establish which parameters contribute most to the variability in system behaviour;
- Derivation of the risk under uncertainty.

Using a Monte Carlo approach, this process typically involves the development of a stochastic system representation of all the interacting processes. This model would be run many times, sampling its inputs from specified distributions of parameter value ranges. The results from this stochastic model must then be statistically analysed to ensure the results from the model are converged, to produce the output distribution and risk calculations.

In addition, sensitivity analysis may be performed to identify those input parameters which contributed most to the variability in the output. These so called sensitive parameters may then be analysed in more detail in order to ensure the results are reasonable, and the model is behaving correctly under extreme conditions.

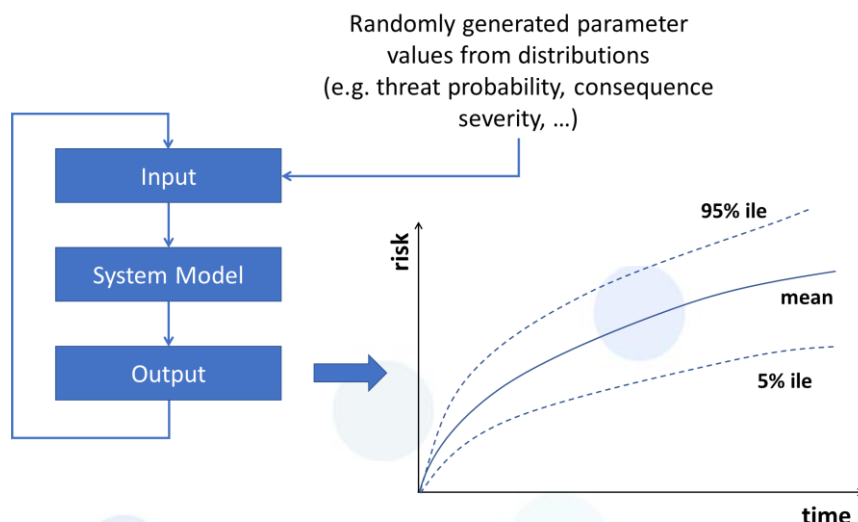


Figure 5-7 - Monte Carlo simulation model

The typical steps in a simulation:

- Establish system model
- Determine probabilistic variables
- Determine probability distribution for these variables a) historical data, b) Derived data (from experts)
- Statistical distribution and parameters
- Check for possible correlation across variables
- Run the simulation

### 5.2.5 Fuzzy logic models

Fuzzy logic (Hossen K., 2013) caters for imprecise information and it is useful for analysing risks when insufficient knowledge or imprecise data exists. Fuzzy logic models, are built upon fuzzy set theory and fuzzy logic.

It allows vague and imprecise knowledge to be processed precisely. Terms such as 'very fast', 'fast', medium, 'slow', 'very slow', can be used to describe continuous, overlapping states. This enables qualitative and imprecise reasoning statements to be used within rule-bases to produce simpler, more intuitive and better-behaved models.

Fuzzy logic is based on the principle that every crisp value belongs to all relevant fuzzy sets to various extents, called the "degrees of membership". As in probabilistic reasoning, these range from 0 to 1. This contrasts with conventional, Boolean (true or false) logic. Allocating membership to sets with values from 0 to 1 enables smoothing and overlapping of boundaries between sets. Unlike Boolean logic where sets are mutually exclusive, fuzzy logic allows crisp values to belong to more than one fuzzy set. This means that whereas in a crisp system, only one rule might be fired and used, in a fuzzy system multi-rules are used, each having influence on the output proportional to its critical membership.

Fuzzy logic systems help simplify large-scale risk management frameworks and can help model the cause-and-effect relationships, assess the degree of risk exposure and rank the key risks in a consistent way, considering both the available data and experts' opinions. It can also provide consistency when modelling risks with limited data. Fuzzy logic recognizes the lack of knowledge or absence of precise data, and it explicitly considers the cause-and-effect chain among variables

Rather than a direct input for the likelihood and potential severity of a risk event, it encourages human reasoning from the facts and knowledge to the conclusion in a consistent and well-documented way.

### 5.3 CONCLUSIONS

In conclusion the DRA for public event depends strongly on a thorough identification of all the hazards and threats during SRA. The assessment should include dynamic hazards that can occur during the event. The identification can be assisted using scenarios generation, what if analysis, event trees, fault tree assessment, or elicitation from experts. The expert elicitation should be able to elicit information on the likelihood of hazards and their consequences. Using a qualitative approach, e.g. a Boston square, the risk can be evaluated. Any identified risks above the risk criteria should be mitigated and procedure to control such risks, should be produced and tested. When the hazards or threats are associated with large uncertainties, more sophisticated methods of assessment should be considered. This could be graphical Bayesian techniques, graphical belief networks (Coppola, 2006), Monte Carlo simulation or fuzzy logic models.

Obviously as the method of assessment becomes more sophisticated, the amount of data requirements increases. The need for more complex models for risk assessment will be only necessary in specific cases when consequences may lead to a large amount of fatalities and casualties or time dependent events changing rapidly and used mainly in the pre-planning and planning stages of the assessment.

For the preparation, planning of a public event and its monitoring, a time dependent GIS could be used which could encompass all the facts including time dependent (possibly geo-located) alerts about the event and could act as a safety management system.



## 6 LETSCROWD APPROACH TO DYNAMIC RISK ASSESSMENT

### 6.1 THE RISKS CONSIDERED IN LETSCROWD

#### 6.1.1 The risks and related threats

The risks to be considered when dealing with mass gathering events are, first of all, those generated by the typical **hazards presented by the crowd and the venue** (UK Health and Safety Executive, 2000):

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

These hazards are not at the core of LETSCROWD, that concentrates on the security threats, but need to be considered since they may intervene after a security threat manifests, influencing the severity of the consequences for the crowd (possible cascade effects).

Then it is necessary to consider all the possible **security threats** related to mass gathering events, including:

- **Terrorism**, that can manifest itself through a (squad of) suicide bomber(s), a vehicle used as weapon, a car bomb, etc., as demonstrated by recent attacks (truck driven into the Berlin Christmas market on 19/12/2016, truck driven into crowd celebrating Bastille day in Nice on 14/7/2016, the multiple shooting and grenade attack in Paris at Bataclan on 13-14/11/2015, etc.).

The advice on a national terrorist risk level, to which an organiser of public event should be prepared for, can be obtained from national advice services (e.g. from MI5<sup>10</sup>). Typical terrorist risk levels and corresponding response levels (as per UK MI5) are described in Table 9 and Table 10, respectively.

<sup>10</sup> <https://www.mi5.gov.uk/threat-levels>

**Table 9 - Terrorist risk levels**

Level	Definition
Critical	An attack is expected imminently
Severe	An attack is highly likely
Substantial	An attack is a strong possibility
Moderate	An attack is possible, but not likely
Low	An attack is unlikely

**Table 10 - Terrorist response level**

Response Level	Description	Threat Level
Normal	Routine protective security measures appropriate to your event	Low and Moderate
Heightened	Additional and sustainable protective security measures reflecting the broad nature of the threat with specific business vulnerabilities and judgements on acceptable risk	Substantial and Severe
Exceptional	Maximum protective security measures to meet specific threats and to minimise vulnerability and risk	Critical

- **Lone wolf terrorist.** The Congressional Research Service offers this definition of lone-wolf terrorism: *"Lone wolf terrorism involves terrorist attacks carried out by persons who (a) operate individually, (b) do not belong to an organized terrorist group or network, and (c) whose modi operandi are conceived and directed by the individual without any direct outside command hierarchy"* (Spaaij R., 2010). There are several types of lone wolf terrorist such as: religious, secular and single issue lone wolf. The research behind lone wolf terrorism tries to answer several questions: motivation of lone wolfs, what are the main issues in fighting a lone wolf terrorist, and what counterterrorism can be used in lone wolf terrorism. The present risk assessment is dealing with identification of different hazards and threats and as such considers only the effects of a lone wolf on safety of the public attending an event. The major challenge is to listen to any police information and any additional information emanating from weak signals. The risk from such attacks increases across Europe and USA and therefore a procedure to deal with such attacks should be developed and verified. This should include rapid response units to reduce the response time from confirmation to tackling such an attack.
- **Domestic extremism**, i.e. individuals or groups that carry out criminal acts in pursuit of a larger agenda, such as "right-wing extremists" or "religious sects". Examples of domestic extremisms have been the "Brigate Rosse" in Italy, "Rote Armee Fraktion" in Germany, ETA in Spain, IRA in Great Britain, etc.
- **Clashes between different groups** participating to the same event (e.g. hooligans of two different football teams, representatives of two different political parties, antagonists, etc.).
- **Insider.** As reported in (Stratton, 2013) *"An emerging challenge for mass-gathering health and medical preparation is the threat of violent sabotage during an event. While terrorism should be considered a form of sabotage, the term "terrorism" is not broad enough to include all the facets that should be considered when preparing for potential violent disruption of a mass gathering. Terrorism implies a systematic use of emotional or physical violence to achieve a recognized end. On the other hand, the broader term "sabotage" includes violent and intimidating acts that lack systematic characteristics and have poorly-defined end goals"*.

Each of the above threats can manifest itself in different attack modes. The following Table 11 represents a tentative to categorise the different possible way in which a threat may occur in order to successively identify which are the possible sources of information that could reveal precursors of that threat.

**Table 11 - Threats to mass gathering events**

Threat	Attack mode	Example from past events
Terrorism	(Squad of) Suicide bomber(s)	Brussels airport attack on 22/3/2016, Mogadishu suicide truck bomb on 14/10/2017, Manchester arena on 22/5/2017
	Vehicle used as weapon (vehicle ramming)	Truck driven into crowd in Berlin Christmas market on 19/12/2016, celebrating Bastille day in Nice on 14/7/2016, van into pedestrians in Barcelona on 17/8/2017
	Car bomb	London car bombs (discovered and disabled before they could be detonated) on 29/6/2007
	Bomb/IED in an abandoned object	Boston marathon bombing on 15/4/2013 Madrid bombings (Atocha and other 3 stations) in March 2014
	CBRN attack	The chemical attack in the suburbs of Damascus (Syria) in which more that 1400 civilians have been killed by a nerve agent in August 2013.
	Cold steel (e.g. stabbing)	London Bridge attack in London on 3/6/2017
	Hijacking of social networks	Nothing similar has yet happened, but the panic generated by a tweet from a pop singer with more than 8000 followers announcing gun shots in a mall <sup>11</sup> is suggesting this a potential terrorist scenario.
	Shooting	Île-de-France attacks on 7-9/1/2015, Jewish Museum in Brussels on 24/5/2014
Lone wolf terrorist	Combined attack (two or more attacks simultaneously launched against the event)	Multiple attacks in Paris on 13-14/11/2015
	Car bomb	Anders Breivik car bomb in Oslo centre on 22/7/2011
	Cold steel	British-born Khalid Masood drove into pedestrians, killing at least two people, before stabbing to death an unarmed officer outside parliament in March 2017. Islamic State claimed responsibility for the attack, but it was not clear whether the attacker was directly connected to the jihadist group <sup>12</sup> .
	Shooting	Anders Breivik shooting in Utøya island on 22/7/2011
	IED	Ted Kaczynski (a.k.a. Unabomber) that between 1978 and 1995 mailed or hand-delivered a series of increasingly sophisticated bombs

<sup>11</sup> <http://www.telegraph.co.uk/news/2017/11/24/oxford-circus-station-evacuated-armed-police-respond-incident2/>

<sup>12</sup> <https://www.reuters.com/article/us-britain-security-response/uk-honed-attack-response-but-feared-unsophisticated-lone-wolf-idUSKBN16U2O5>

Threat	Attack mode	Example from past events
Domestic extremism	Car bomb	Omagh bombing on 15/8/1998, Hipercor bombing in Barcelona on 19/6/1987, bomb at Uffizi gallery in Firenze on 27/5/1994
	Cold steel	
	Bomb in an abandoned object	Piazza Fontana explosion on 12/12/1969
	CBRN attack	Tokyo subway sarin attack on 20/3/1995
	Shooting	Las Vegas shooting on 1/10/2017
Clashes between different groups	Riot	The 2012 European Men's Handball Championship riots, where a group of Croatian fans who were heading home were attacked by 50 masked men with axes, stones and bricks, and a fan was stabbed
		The 2007 A.S. Roma–Manchester United F.C. conflict, when groups of fans started throwing missiles over a barrier that was to separate the fans, prompting Italian riot police to enter the stadium
		Football fans riot on streets after Feyenoord miss chance to win Eredivisie title on penultimate day in 2017 in The Netherlands.
	Cold steel	Two Leeds fans were stabbed to death the night before Leeds played Turkey's Galatasaray in April 2000.

Other possible threats that never occurred but that have been identified as potentially possible are:

- Vehicle ramming attacks in the age of driverless cars by hacking autonomous vehicles (Woodhouse, 2018);
- Weaponised drones<sup>13</sup>;
- Spread of infectious diseases (World Health Organisation (WHO), 2015).

The following Table 12 proposes possible precursors for the threats identified in Table 11 with the aim of putting them in relation with the weak signals described in Section 7; this list does not pretend to be exhaustive but to offer a first survey of possible precursors that can grow with project's life.

The sources used to identify the threat precursors are heterogeneous ranging from news of past events, governmental reports or web sites<sup>14</sup>, academic journals, conferences, LEAs' feedback, Deliverable D3.1, etc.

The list starts from the terrorist threat that intrinsically generates the majority of precursors and is then completed by all other threats avoiding repeating similar precursors for each considered threat.

<sup>13</sup> <https://www.theguardian.com/commentisfree/2018/jan/19/terrorists-threat-weaponised-drones-swarm-civilian-military-syria>

<sup>14</sup> <https://act.campaign.gov.uk/>

**Table 12 - Threat/precursors table**

Threat	Precursor(s)
Terrorism	Filming, taking notes or photographs, or watching for extended periods, focusing on security cameras, hallways, fire exits, access and egress routes
	People behaving strangely, e.g. nervous, perspiring, wearing overly warm clothing, concealing their face, repeatedly patting upper body parts, etc.
	People bringing unusual packages into your event (e.g. a disproportionate weight of luggage considering its size)
	People found in off limits areas, particularly near plant or server rooms or places of concealment
	Vehicles parked in suspicious circumstances
	Anomalous vehicle e.g. a vehicle with different front & back license plates, with apparent heavy weight on rear axle, with large containers or gas containers inside, with additional visible improvised electrical wires
	Anyone buying or storing a large amount of chemicals, fertilisers or gas cylinders for no obvious reasons
	Social network activities including, for example, hatred, admiration to terror causes, posting pictures or information regarding traveling to known terror training and recruiting locations, explore different terror or radical organizations, strategies and tactics, explore acquisition or construction of weapons or dual use materials, seek out, read, or post radical content, release information or discuss in social network how to harm or influence target
	Splitting into groups (signalling multiple points of attack)
	Identical luggage carried by several persons
	Abandoned object
	Cyber-attack to critical infrastructures (e.g. denial service of telecommunications of rescue teams before an attack)
Domestic extremism	Mobilisation via social media, e.g. efforts to "Unite the Right" in Charlottesville - USA (Peterson J., 2017)
Lone wolf	Signs of radicalisation on social media <sup>15</sup>
Clashes between different groups	Group of many persons with similar symbols (clothing, flags, etc.)
	Mobilisation via social media

### 6.1.2 The likelihood of the threats

The risks considered in Section 6.1.1 are considered "High Impact Low Probability Risks" - with the exception of the clashes between different groups<sup>16</sup> - and therefore managed accordingly (UK Government Office for Science, 2011).

Therefore, as reported in (Willis H.H., 2005) *"When facing uncertainty about estimates and values, policy analysis often relies on best estimates, even when they have a low probability of being correct—and a high probability of being wrong. While this allows us to generate a very precise estimate of risk, in the end, if the*

<sup>15</sup> E.g. A. B. Breivik used several different social networking sites such as Facebook and Twitter and posted his manifesto "2083, A Declaration of Independence of Europe" on the Internet (43)

<sup>16</sup> In the case of risk of clashes between different groups, LEAs have already in their databases many records of past events from which to derive statistics on likelihood of clashes: this is true for both extreme (left or right) political organisations, sport fans, etc.

*estimates poorly represent what actually happens in real life, the precision is misplaced. So, rather than seek an optimal method for estimating risk, we seek a method that leads us to make the least egregious errors in decision-making across the range of possible scenarios that might develop in the future".*

So Dynamic Risk Assessment (DRA) methodology should help LEAs in **dynamically assess the risks** on the basis of the **dynamically collected information** to minimise errors in decision-making across the range of possible scenarios that might develop at the event venue.

## 6.2 THE DIFFERENT PHASES TO ASSESS RISKS FOR MASS GATHERING EVENTS

The assessment of risks for mass gathering events typically develops along 3 different phases as defined in Deliverable D2.2, section 2.2.4 (LETS-CROWD project, 2017):

- **Event Preparation**
- **Event Execution**
- **Post Event**

The Event Preparation phase can be then further subdivided into 2 different stages:

- **Early Planning**, in which the decision to organise the event is taken and in which risks are statically assessed (see Section 6.2.1);
- **Pre-Event**, in which the decision to organise the event is taken, participants are not yet present at the venue and organiser and LEAs are putting in places all the possible measures to guarantee safety and security (see Section 6.2.2).

The sequence of the phases is shown in Figure 6-1; the 4 phases differentiate themselves for

- The time that separates the stage from the mass gathering event.
- The amount of available information, the trustability/reliability of the collected information and related tools to process it.
- The possible consequences for the crowd.
- The available reaction time for LEAs to sense information, process it, evaluate potential threats and related risks, act and mitigate them.



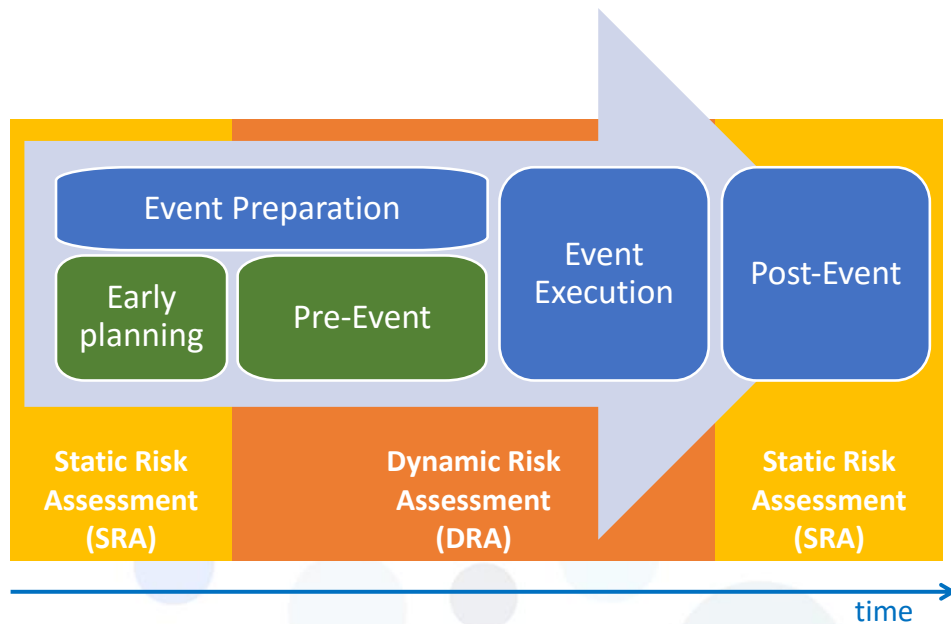


Figure 6-1 - The Static & Dynamic Risk Assessment stages

The characteristics of the different stages are described in the following sections.

### 6.2.1 Early Planning

In the **Early Planning** stage, the organiser decides to plan for an event that will gather crowd in a given venue. In this phase the organiser, quite often together with the involved LEAs, implements a traditional risk assessment. This phase is essentially a **Static Risk Assessment (SRA)** activity: there is no real-time information flow and all assessments and decisions are taken on the basis of existing data, standards and good practices, geomorphological and architectural characteristics of the venue, experience of involved stakeholders, and lessons learnt from past similar events (UK Health and Safety Executive, 2000), (Raineri, 2015), .

This stage takes place typically at least some weeks before the date of the event.

### 6.2.2 Pre-Event

In the **Pre-Event** stage, the nature of the threats is still unclear, and the LEA's operational mode is as defined in directives and regular operational SOP's.

This is a relatively slow **Dynamic Risk Assessment** phase (see Figure 6-2 for a flowchart of the process) in which LEAs and organiser, starting from the static risks assessed in the Event Planning stage, must:

- **Listen to all possible weak signals** potentially related to the security of the event and identify the possible threats associated to them for which many different weak signals could be considered as precursors.
- Try to **process (correlate) the different weak signals** in order to see if they can contribute to increase or decrease the level of each related risk.
- **Dynamically update the risk levels** according to:
  - Whether the collected **weak signals** information is correlated,
  - Whether the **unforeseen events** occur during the event preparation.
  - The new **intelligence information** is generated and gathered in this phase.
- **Manage the uncertainty** associated with the different possible risks.

- **Whether they modify** the risk level.
- **Re-plan the mitigation measures** according to the modified risk levels.

In this phase all possible risks are assessed and managed, independently of their level.

The possible approaches to process and manage weak signals are described in Section 7.5 while the weak signals considered in LETSCROWD are reported and analysed in Sections from 7.1 to 7.4.

The Pre-Event stage lasts from the end of the Early Planning Phase until the point at which **LEAs start to enact the plan** (for example when the first person arrives in the boundary of the event, or when LEA officers are in place ready for the event - this could be a number of hours before the start of the event). Therefore, LEAs and organiser have time for reactions and therefore enough time to run models and simulations as well as relatively complex algorithms for correlating/fusing in space and time the different sensed weak signals.

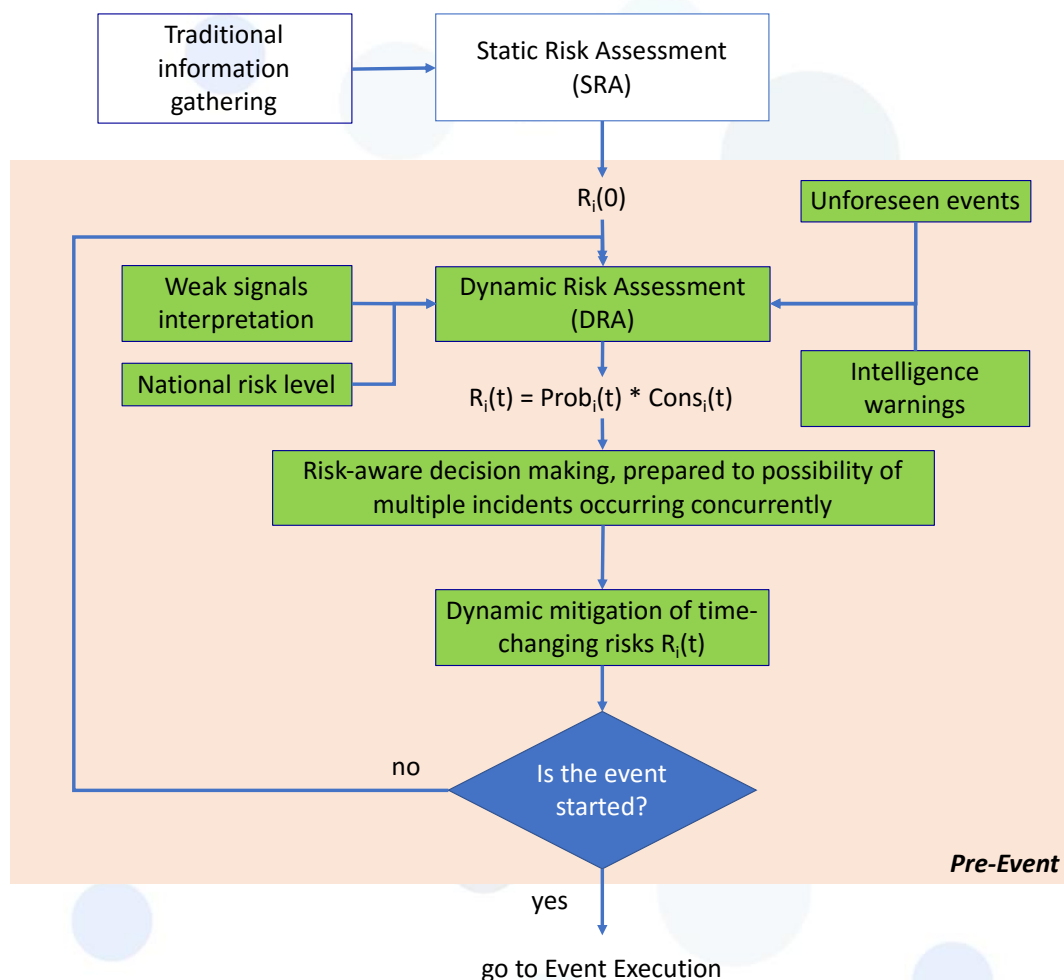


Figure 6-2 - The approach for the Pre-Event stage

At this stage all the hazards which can occur during the public event are postulated considering the venue duration time and the site characteristics. The assessment should consider the number of entrances to the event and evaluate the maximum rate of ingress and egress that each of the entrances/exits can accommodate. Also, what type of crowds the organisers are expecting and its size. Other issues to consider are the routes to the event, whether there are any dead ends, locked gates, uneven surfaces etc. and how

the flow of people may affect potential for injuries. The SRA must feed information on the identified risks and any procedures related to dealing with such risks.

The possibility of terrorist attacks on the public and the consequences of their action should also be analysed considering any intelligent reports. If the results of risk assessment indicate possibility of terrorist attack, the plans for the event should consider how to carry out effective searches for possible bomb threats, and means of looking for suspect packages, cars etc.

The plans for evacuation of public from different parts of venue to mustering and identified shelters and evacuation routes should be considered and procedures for how to deal with such threats assessed.

The list of hazards and their risks identified as feasible should be stored in the event database and risk log together with the procedures for their reduction or elimination if they occur.

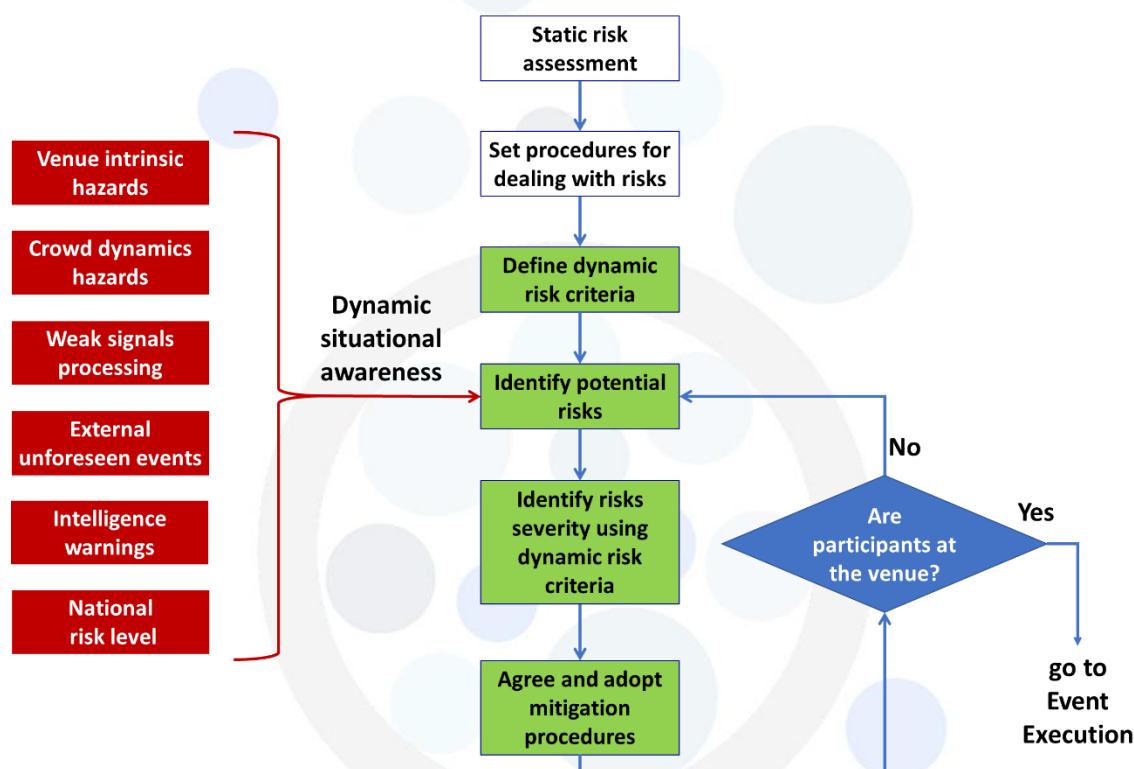


Figure 6-3 – Pre-Event risk assessment steps

The dynamic risk assessment for possible hazards which may occur during the event are next postulated (Allen, 2012). The effect of weak signals on risk has already been discussed in this chapter. How they will be assessed, combined together from different sources, ensures that they can be verified, and appropriate action taken. All the time dependent hazards should be systematically considered on the basis of timeline of the venue, i.e. from the time the public will start to gather to the venue, until their departure and dispersal. The rest of methodology presented on Figure 6-3 is similar to method applied for static risk assessment. The mitigation applied to DRA should be practical and readily applicable in a dynamic situation. The most effective mitigation is the training of the personnel involved in the control of the event. They should be familiar with the risk assessment results, applicable procedures and understanding safety condition as applied to the public venue.

### 6.2.3 Event Execution

Event Execution phase differs from the previous phases for a fundamental element: the **presence of the crowd**.

The presence of the crowd modifies the way in which involved stakeholders may act:

- Having the presence of the crowd obliges the LEAs to act immediately whenever a threat manifests to minimise, **As Low As Reasonably Practicable (ALARP)**, the consequences for the participants to the event.
- As a consequence of the above,
  - Only **risks above a predetermined threshold** are considered and focus will be concentrated on possible related mitigation measures.
  - Only **real-time tools** can be used, thus limiting the risk assessment to simplified predetermined scenarios.
- The main sources of information that contribute to the Dynamic Situational Awareness will be:
  - Details on unforeseen events from reliable sources.
  - Very reliable sensors (e.g. the policemen at the event venue or the specifically trained organiser's stewards).
  - Intelligence warnings.

The dynamic hazards may rise during the three phases of the Event Execution stage (see Section 6.2.3) of the event:

- **Ingress** of people to an event
- **Circulation**: people movements during the event
- **Egress** of people from the event.

During the ingress or egress of people entering or leaving the event, with larger rates than planned, could give rise to dynamic risks from pushing, when enlarged queues are forming.

In this stage the involved stakeholders (LEAs, the organisers of the event and their marshals, etc.) are watching for any hazardous or threatening event.

Hence referring to Figure 6-4, the procedure can be summarised as follows:

- 1) New hazard or threat is identified. The safety controller checks whether procedures to deal with this hazard exist. If the hazard has been already identified, the method of dealing with this hazard follows the procedure for dealing with it. If, however, this hazard had not been previously identified, the safety controller should try to identify a similar hazard from its database.
- 2) If the existing control for the similar risk is adequate, then proceed with procedure for dealing with this type of risk.
- 3) If the mitigation for this new risk is not adequate, check if any additional mitigation is possible from controller experience. If not, consider risk to be intolerable and activate procedure for intolerable risk including mustering and evacuation.
- 4) If additional risk control is possible, then check if adequate and proceed with mitigation procedure for this risk.
- 5) If additional risk is not proven, consider the risk as intolerable and activate procedure for intolerable event.

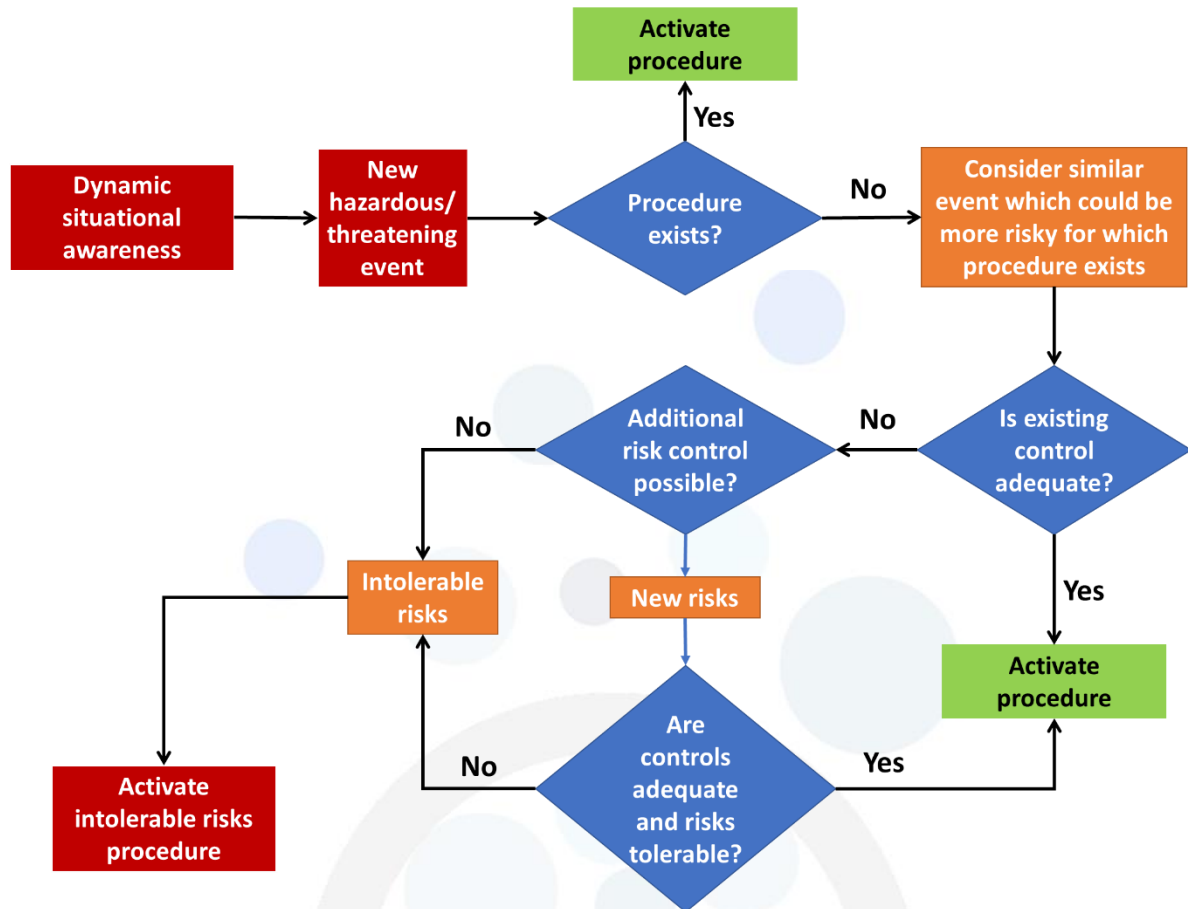


Figure 6-4 - Event Execution process

Such a methodology depends on identification of all critical hazards, risks in a planning stage and having the right procedure to deal with most of the risks as function of time. It also assumes that the people in charge of the event have the right training in safety and dealing with a large number of people.

## 6.2.4 Event Closing and Assessment

The key activities involved in the closing stages of an incident are:

- Maintaining control;
- Incident Debrief;
- Review effectiveness of the applied mitigation controls;
- Collect key information for further analysis.

## 7 ANALYSIS OF EXISTING SENSED WEAK SIGNALS

The Dynamic Risk Assessment approach relies, amongst the various inputs available, on the interpretation of weak signals considered in LETSCROWD (see Section 6).

In this section, the different weak signals are briefly analysed in order to understand their possible contribution to the Dynamic Risk Assessment and, in particular, if and how far they can be considered precursors of identified threats.

The following sources of weak signals are considered in the following:

- Cyber-Threat Intelligence.
- Semantic Intelligence.
- Human-Centred Computer Vision.
- Human as a Sensor.

### 7.1 CYBER THREATS INTELLIGENCE ON MASS GATHERING EVENTS

Cyber Threats Intelligence (from now onward simply CTI) main focus is on providing “intelligence” but this depends on the filtering and aggregation of smaller pieces of information that comes from different sources. CTI can be divided into different “branches” according to the kind of source used to gather the starting information. While in the end, the final intelligence provided to the decision makers will be derived from all possible, and available sources, is still useful to clarify what different kind of “intelligence” we are able to generate according to the source of the gathered information:

- Open Source Intelligence (OSINT) – open sources available on the web.
- Social Media Intelligence (SOCMINT / SMI) – social media platforms, open and closed.
- Human Intelligence (HUMINT) – human beings (e.g., interrogation, wiretapping, elicitation, etc.).
- Technical Intelligence (TINT) – sources from the deep web and dark web.

These sources of information, and subtypes of CTI, can be considered valid even in the specific case of “mass gathering events”. Let’s consider some possible scenarios labelled, for the sake of simplicity as “digital” and “physical”:

- **Digital Scenario** – A mass gathering event can be the “opportunity” for an attacker to launch an attack against digital infrastructures and devices owned by private and public companies (i.e., not necessarily related to the event) or by people attending the event. The attack itself is performed against digital assets and/or it is mostly based on technical expertise. Some examples of this scenario are phishing campaigns that leverage the event (e.g., free tickets, fake news about the event, etc.), installation of hardware to target mobile devices of attendants (e.g., IoT WiFi spots with fake “official” names for large scale attacks), etc.
- **Physical Scenario** – A mass gathering event can be used by an attacker to perform a terrorist attack. In this context the attack is not “cyber” and is completely “physical” and it happens in real world. In this scenario the CTI can be useful to spot Weak Signals of an incoming attack. As an example, it can be considered useful to monitor certain websites and forums where “criminal knowledge” is shared (e.g., guides to create and handle explosives, guides on how pick locks or use guns), to monitor the “behaviour” of certain individuals on social media (e.g., sentiment analysis applied to text, sharing contents such as pictures of weapons, peaks of activity, etc.).

The following Table 13 shows what is the role of the “cyber” part in both scenarios for both the attacker and the defenders.



**Table 13 - The role of “Cyber” in the scenario**

	Attacker Side	Defender Side	CTI Side
Digital Scenario	The performed attack requires either technical expertise or an acquired set of tools (e.g., malware such as RAT or APT, Zero-days exploits, etc.) built from experts. In a real scenario the attacker needs at least average skills even to use acquired tools. Not just that the tools are “digital” but also the targets (e.g., server, mobile devices, IoT devices, etc.).	The nature of the targeted assets makes it is necessary to deploy “digital defences”. Not just hardware (e.g., firewall, encrypted hard drives) and software (e.g., IDS, secured communication protocols) but also methodologies (e.g., Application threat modelling, operational threat modelling).	CTI can initially be used to model the system and deploy the best possible defences. Then to monitor the assets for any sign of an incoming attack. During an attack CTI can be used to decide the best approach to slow down or block the attack. Once the attack is over (i.e., complete or blocked) CTI can help gathering evidences for legal purposes or to improve the defences of the system.
Physical Scenario	The attack does not require IT related skills to be performed. If a highly technological tool is involved, it does not require specific skills to be used. Attackers can use the web to gather information, to train themselves (e.g., learn how to make homemade bombs), for an internal communication (e.g., chat groups, social media platforms) or to communicate with the world (e.g., share a political/religious “manifesto”, claim their involvement in the attack).	The attack is not carried out against digital targets but there could be “minor” targets involved (e.g., cameras that monitor the location of the attack, antennas used by defenders to communicate). Furthermore, preventing and monitoring the actions of the potential attackers on the web can provide information on their strategies (i.e., thus improving the defences) and reduce the effectiveness of their attacks.	CTI can be used to monitor the amount of information available to attackers (e.g., measure how much useful information for the attackers is available on open sources) but also to monitor the activity of attackers on social media (e.g., number of groups and chats used, number of users, number and frequency of messages). Behavioural analysis and natural language processing can be useful to “profile” the targets or to filter the collected information. These kinds of activities can be severely limited by technical, legal and ethical boundaries.

This introductive paragraph does not aim to provide a complete set of real attack scenarios but only to highlight how CTI involvement in dynamic risk assessment changes depending on the type of scenario we consider. This is extremely helpful in defining what kind of Weak Signals are important and what are the sources of information that should be taken into account.

Usually CTI puts great focus on collecting information, but this is only the first step of a long complex process that aims to turn that information into intelligence. Beside all the possible legal, ethical and technical

difficulties of collecting the information (e.g., Terms of Services of the social media platforms, handling huge amounts of data, etc.) there are also other inherent problems:

- **Data size and threat prioritization:** the amount of data that can possibly be collected is huge, and important pieces of information are hidden among “noise”. It is fundamental to focus on the most important threats... but what are they? Prioritization is hard but necessary.
- **Mapping information to indicators:** in order to provide “intelligence” it is required to provide some real indicators that can be monitored. Attacks against digital infrastructures can use typical indicators used in cyber security while more “physical attacks” (e.g., terrorist attacks, riots, etc.) can leverage more psychologically oriented indicators based on target behaviours.

Continuing with the previous example of two scenarios, one more “digital” and more “physical”, it is now the time to focus on what type of indicators, or weak signals can the CTI focus on.

**Digital Scenario:** In the past years, security experts focused on the signals known as *Indicators of Compromise* (IOC) while now is more common to focus on *Indicators of Attack* (IOA). Unlike the IOC, IOA focus on detecting the intent of what an attacker is trying to accomplish, regardless of what technical approach (e.g., malware, exploit) is actually used in the attack. An IOA represents a series of actions that must be performed in order to succeed. IOAs are concerned with the execution of these steps, the intent of the adversary and the outcomes he is trying to achieve. By monitoring these execution points, gathering the indicators and analysing them, is possible to determine what is happening to the network in real time. The targets need to face “adversary problems” and not “malware problems”. By the time an IOC has been detected, the attack is already ongoing and maybe even complete.

**Physical Scenario:** IOA and IOC are not well suited to this scenario since, as previously stated, the main target of the attack is not a digital asset. The approach based on IOA can be useful if the indicators are based on a broader range of disciplines (e.g., social sciences, finance, etc.). For example, Cohen (Cohen K., 2014) suggests a list of behavioural markers for radical violence that can be extracted from written text, Meloy (Meloy J.R., 2012) provides and even broader range of markers for “warning behaviours”. Other interesting indicators can focus not on the “intent” of committing or being part of a violent act but also on radicalization and “bonding”. According to Fredholm (Fredholm, 2011), nearly all radicalization of “lone wolf terrorists” takes place on the Internet. According to Sageman (Sageman, 2008), the lone wolves are actually “lonely” only in real life while on the “web” most of them are part of communities (e.g., forums), this is especially true for those lone wolves that actually carry out attacks. As an example: Anders Behring Breivik used several different social networking sites such as Facebook and Twitter and posted his manifesto “2083—A European Declaration of Independence” on the Internet before committing the two terror attacks in Norway.

### 7.1.1 Weak Signals for the Digital Scenario

Plenty of weak signals can be potentially collected in this case but their definition requires a prior threat modelling process. Usually IOA are based on a previously performed threat modelling, a practical process by which organizations can be proactive in their security efforts. Threat modelling can be divided into two processes:

- **Application Threat Modelling:** focuses on the application/service itself as created by the development team.
- **Operational Threat Modelling processes:** focuses on the underlying operational infrastructure – the servers, databases, load balancers, and other such infrastructure components – that constitute the operational environment in which this application will operate.

In order to fully consider risk mitigation for this application, both aspects must be addressed in accordance with their own unique concerns. Performing these processes does just “mitigate the risk” but also provides a list of IOA or Weak Signals that can be used to monitor the assets and spot an incoming attack.

**Application Threat Modelling** – It starts with the creation of a Process Flow Diagram (PFD) in order to allow developers, security professionals and stake holders to build a model of what is a “normal” flow of actions performed by a legit user on the application. The PFD helps in creating Weak Signals such as a set of “correct” sequences of actions. Any activity that does not fall into these list is either the result of an error from the system or some malicious activity. Note: these sequences can be used together with AI based IDS.

**Operational Threat Modelling** – it focuses on the end-to-end data flow of the organization’s infrastructure. It starts with the identification of all “environments”, including shared components (e.g., servers, switches, etc.), then it continues with the gathering of information about each component (e.g., a certain server contains sensible information, another one has a specific restricted access policy, etc.) and finally it focuses on known vulnerabilities (i.e., CVE) for all involved components. This modelling provides with plenty of possible interesting pieces of information such as:

- Number and severity of CVE
- Following of standard best practices in computer security (e.g., access level, encryption, etc.).

These can be mapped to Weak Signals such as:

- Patterns in Incoming network messages.
- Increased interests in underground forums about tools and strategies that can be used against the system.

The current trend in cyber security and CTI is to collect and document IOA (i.e., and IOC) in a common open format known as STIX<sup>17</sup>. Collected knowledge can be then shared and transferred using a special protocol known as TAXII<sup>18</sup>. The rationale behind this trend is to improve the quality of Weak Signals by sharing them and also increase the resources of “defenders” by pooling together the result of different CTI teams together<sup>19</sup>.

### 7.1.2 Weak Signals for the Physical Scenario

Some useful weak signals can be potentially collected using information gathering and data analysis methodologies and tools. This is a list of weak signals based on the work of Maloy (Meloy J.R., 2012) and Cohen (Cohen K., 2014); they focus more on the “lone wolf” cases but can be considered a starting point for other scenarios too:

- Being active on a “radical” web page.
- Use of “radical expressions” in communication on social media.
- Leakage.
- Identification.
- Fixation.
- “Energy burst” warning behaviour.
- “Last resort” warning behaviour.

The following paragraphs describe each of the proposed weak signal.

**Being active on a “radical” web page** – the fact that someone is active on a radical web page can be revealed by identifying any kind of activity performed by the given user on any “page” that belongs to an existing list

<sup>17</sup> <https://oasis-open.github.io/cti-documentation/stix/intro>

<sup>18</sup> <https://oasis-open.github.io/cti-documentation/taxii/intro>

<sup>19</sup> <https://oasis-open.github.io/cti-documentation/>

of relevant “pages”. This weak signal requires a list of web pages (i.e., from website and blogs), social group (e.g., Google+ circles, Facebook groups and pages, etc.), forums, etc. This list can be manually or automatically compiled but must contain “pages” that are considered to be “radical” in some sense. The assumption that everyone that is “active” on these pages must be an extremist does not necessarily hold true but can be an interesting indicator, especially if other indicators are positive too.

**Use of “radical expressions” in communication on social media** – classifiers for the estimation of a “level of radical content” in a body of text can be built in various ways. Different technical solutions are possible with trade-offs in regards of the requirement of manual inspection, the presence of a starting dataset, computational requirements, minimum length of the text required for an analysis. According to the chosen solution the accuracy can change.

**Leakage** – according to Semenov and other researchers (Semenov A., 2010), school shooters (i.e., a phenomenon closely related to “lone wolf terrorism”) have the notable characteristic of announcing their views and intentions in advance. It seems that most perpetrators revealed their intentions in social media before actually carrying out their attacks. Leakage is defined as the communication to a third party (e.g., a group of people on a social media platform, chat users, etc.) of the intent to do harm to a “target”. It should be noted that Leakage can be intentional or unintentional and more or less specific (Meloy J.R., 2012).

**Identification** – this warning behaviour is defined as the desire to be a “pseudo-commando”, to have a “warrior mentality” or to be closely interested in paraphernalia usually associated to military or law enforcement agencies. This warning behaviour is also manifested in the desire to be identified with previous attackers/assassins or in the self-identification in an agent that aims to advance a particular cause (Cohen K., 2014). This definition is quite broad because of the complexity of the phenomenon. According to (Meloy J.R., 2012), is possible to divide identification into two different subcategories:

- Identification with radical action
- Identification with a role model

It should be added that “group identification” is common to both “lone wolves” and groups of organized terrorists. In regards of this Weak Signal, here are some examples of how it is possible to measure it by analysing text written by a given person:

- Identification with a warrior can be revealed by the use of a certain terminology, while a sense of moral obligation can be expressed through the usage of words related to duty, honour, justice, etc.
- Identification with another radical thinker can be revealed by frequent mentioning and quoting and by a similarity of language (i.e., use of similar lexicon, sentence structure). It can be useful to consider the possibility of using author recognition techniques.

**Fixation** – this warning behaviour indicates a focus on a certain person (i.e., a potential target) or a cause (e.g., ethnic cleansing, racial purity, religious war, etc.). It is manifested in the increasing perseveration on the object of fixation, increasingly strident opinion, or increasingly negative characterization of the object of fixation (Meloy J.R., 2012). As a Weak Signal, Fixation can be spotted by the tendency to repeatedly comment on an issue or a person, which in written communication result in an increases frequency of “mentions”. Another approach to spot Fixation is to look for frequent combination of certain key terms that can be associated to a certain idea if found together.

**“Energy burst” warning behaviour** – this behaviour relates to an increase in the frequency or variety of activities related to the target when the day of attack is approaching. This behaviour can result in Weak Signals similar to those associated to Fixation.

**“Last resort” warning behaviour** – this behaviour can be seen as an expression of an increasing desperation or distress, in which the individual sees no way out except by taking violent action.



It is interesting to point out that, while some of these behaviours are more likely to be detected using physical interaction, many of them can also be identified by activity on social media platforms and, by extension by other kind of internet related activities. Some of these behaviours are related to the capability to carry out an attack, others to the intent of doing it while others focus on the opportunity to carry it out. Natural language processing can be used to analyse text written in order to spot relevant behaviours; social media analysis can also be useful (e.g., a person is part of groups that focus on weapons, war, racism, religious wars, etc.); image recognition applied to media (i.e., images and videos) shared on media platforms can be useful too (e.g., a person takes a “selfie” while posing with a weapon).

## 7.2 SEMANTIC INTELLIGENCE

### 7.2.1 Social networks and possible threats to mass gatherings events

The recent massive increase in Social Networks use have heavily modified, on one side, the way in which people communicate and, on the other side, the sources of information to be used by LEAs during investigations:

- Social Networks are nowadays used by citizens participating in mass gathering events to quickly **mobilise and organise themselves** into groups. Crawling of this information (often public and therefore without ethical/privacy issues) can be used by LEAs to predict the characteristics of crowd participation to events and therefore analyse potential safety hazards (e.g. overcrowding, inadequate planning by the event organiser, etc.) or security threats (e.g. participation of groups possible targets of terrorist activities, culturally clashing groups, etc.).
- Terrorists are using Social Networks for their **communication, mobilisation and recruitment needs**. However, as it has been recently reported by Laurence Bindner, a Cyber-Intelligence Consultant, in her speech at MILIPOL (Bindner, 2017) jihadists (and, more in general, terrorists) are moving away from traditional social networks (Twitter, Facebook, etc.) towards more anonymous encrypted solutions like Telegram or WhatsApp.

This move makes crawling almost impossible, even if at the European level there is a continuous effort in finding a solution for the increasing challenges encountered by law enforcement and judicial authorities posed by the use of encryption by criminals (European Commission, 2017): *“the following set of measures to support law enforcement and judicial authorities when they encounter the use of encryption by criminals in criminal investigations should be implemented. This includes (a) legal measures to facilitate access to encrypted evidence as well as (b) technical measures to enhance decryption capabilities”*.

- Social media are also widely used to support **violent radicalization movements and ideologies** (both impacting on terrorist and domestic extremism threats) as demonstrated by a recent UNESCO report (S. Alava, 2017) on youth and violent extremism on social media. From the report it is possible to extract the following conclusions that are interesting for the LETSCROWD approaches:
  - *“Internet and social media may play an active role in the violent radicalization process, mainly through the dissemination of information and propaganda, as well as reinforcing the identification and engagement of a (self)-selected audience that is interested in radical and violent messages”*.
  - *“Rather than being initiators or causes of violent behaviours, the Internet (and social media specifically) can be facilitators of radicalization. According to the literature, Internet’s role thus seems more specifically one of decision-shaping rather than triggering decision-making, and it works through the creation of an environment of like-minded people constituted in opposition to an ‘Other’”*.

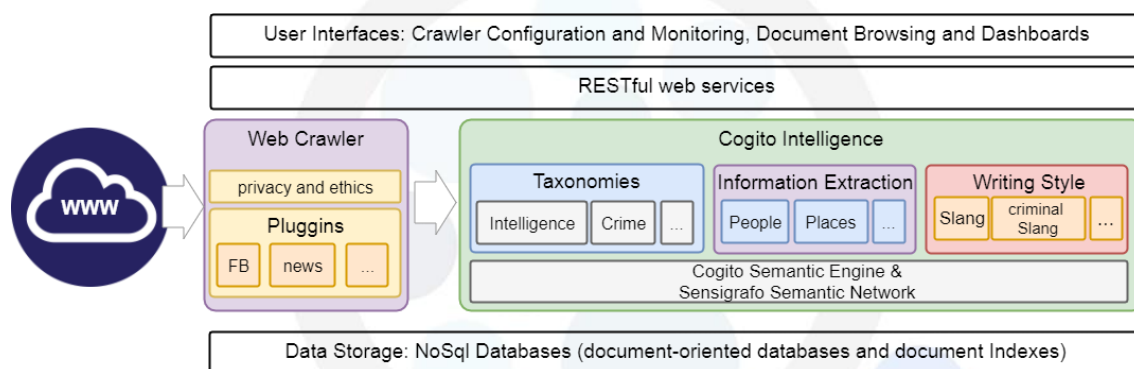
- *“Currently, there is some evidence for correlation between exposure to extremist propaganda and recruitment and the expression of extremist attitudes and increased risk for violent radicalization among youth, particularly in the case of extreme right-wing groups”.*

The above statements can help semantic intelligence to adjust the taxonomies to the violent radicalisation phenomena.

### 7.2.2 The use of semantic intelligence to detect weak signals in social networks

The semantic Intelligence engine enables security analysts to assess threats for mass events from the analysis of large text collections that are gathered from social networks and web sites in general. The tool main components are (see Figure 7-1):

- a focused crawler that extracts text from the Web while guaranteeing the user privacy and web site terms of use;
- Cogito intelligence engine to process the text and enrich it with structured metadata relevant to security analysis such as categories in specialized taxonomies, named entities and their types, and the author's writing style, and
- a set of visualization tools, including search engines and dashboards, that leverage the metadata generated by Cogito to browse, inspect and analyse the document collection from a security perspective.



**Figure 7-1 - Simplified view of the components comprising the semantic intelligence engine**

Statistics about the metadata generated by the semantic engine for a document collection could be considered as weak indicators in the risk assessment methodology. For example, a security analyst set up the crawler to retrieve news, web pages and social posts that mention the event “UEFA champions league final”. If after running the crawling for some days a significant proportion of web contents are classified under the category “Terrorist activities and tactics” in the Terrorism Taxonomy, the security analyst can emit an alert to the appropriate stakeholder with the web contents in the category including their provenance information. Similarly, the security analyst can trigger alerts if the semantic engine recognizes entities of type “terrorist organizations” in a significant number of documents, or that some authors use a slang that is commonly used in criminal contexts.

In the following a short description of the taxonomies and other metadata added to the text document is presented. Please note that deliverable D5.3 presents a full description of the Semantic Intelligence Engine including extended descriptions of the metadata.



### 7.2.2.1 Taxonomies

Cogito intelligence engine classifies text documents in categories pre-arranged in a taxonomy. Currently five taxonomies are supported: Intelligence, Crime, Terrorism, Geography, and Emotions. To perform the classification task the engine has a set of rules per category in each taxonomy that define patterns of information that must be present in the text so that the document can be identified as falling in one category. The built-in taxonomies are:

- **Intelligence taxonomy:** based on the IPTC taxonomy<sup>20</sup> contains around 500 categories in intelligence sector's domains such as arms, intelligence, military, defense, internal security, international security, critical infrastructures
- **Crime taxonomy:** based on the standard model defined under the "Swedish Initiative" (a common protocol and knowledge model which promotes the effective exchange of information and strategic data between EU States' law enforcement authorities) contains 32 categories
- **Terrorism Taxonomy:** covers the terrorism domain with 80 categories targeting its matrixes (motivations), activities, tactics, models, and targets,
- **Geography Taxonomy:** contains 250 categories, where every category represents a country
- **Emotions Taxonomies:** contains 75 emotions and behaviour categories arranged in one level.

To show the metadata generated by the intelligence engine the following example text is used as reference:

*"The Prime Minister of Spain, Mariano Rajoy, called the attack in Barcelona a jihadist attack. Amaq News Agency attributed indirect responsibility for the attack to the Islamic State of Iraq and the Levant (ISIL)."*

In the following an excerpt of the categorization produced by Cogito intelligence engine for this text is presented:

**Table 14 - Categorisation produced by COGITO SW**

Taxonomy	Category1	Sub-category
Intelligence	Crime, Law and Justice	Crime
Intelligence	Unrest, Conflicts and War	Act of Terror
Crime	Terrorism	
Terrorism	Terrorism by matrix	Religiously inspired terrorism
Geography	Spain	
Emotions	Stress	

### 7.2.2.2 Information Extraction: Entities and Types

In addition to classification in taxonomy categories, the intelligence engine can recognize and assign a type to named entities found in the text. The recognition and classification of entities in text are part of a general process known as information extraction from text documents. To recognize and classify entities the semantic engine first spots entities according to the context and then based on a proprietary semantic network assigns a type to the entities. A semantic network is a graph that encodes the domain knowledge by linking concepts and instances of these concepts using linguistic relations such as hypernym, hyponym, is-a, among many others. The complete list of entity types that the semantic engine recognizes is:

- Standard entities
  - People: human proper names
  - Organizations: organizations' proper names

<sup>20</sup> <https://iptc.org/standards/newscodes/>

- Places: places proper names
- Domain-specific entities
  - Biological Agents: bio hazard and substances
  - Chemical Agents: chemical hazard and substances
  - Criminal Organizations: criminal enterprises
  - IP: IP addresses
  - Military Equipment: military equipment and vehicles
  - Most Influential People: influential people's names
  - Military Actions: military actions
  - Natural Disasters: natural disasters
  - Designated Terrorist Organizations: terrorist groups
  - Weapons of Mass Destruction: weapons of mass destruction
  - Infrastructures: critical infrastructures
  - Buildings: constructions names
  - Points of Interest: Points of Interest
  - Most Wanted: names and official aliases of criminals wanted for terrorist activities

Following with the example text the intelligence engine extracts the following entities:

**Table 15 - Extract of the intelligence engine**

Entity	Types
Mariano Rajoy	People, World Leaders
Amaq News Agency	Organization
ISIL	Organization; Terrorist Organizations
Barcelona	Place
Spain	Place

### 7.2.2.3 Writing Style: Slang

Finally, the semantic engine analyses the writing style of the text author and outlines a document's readability and the level of education necessary to understand it. Relevant to our analysis are the percentage of slang used in a document and the type of this slang. The percentage of slang is calculated as the ratio of the number of slang words with respect to the total amount of distinct words in the text. The types of slang supported by the semantic engine are:

**Table 16 - Slang types**

Type	Description
SLANG	Words and phrases that are regarded as very informal and often restricted to special context
CRIMINAL_ENTERPRISE_SLANG	Slang used in criminal context
CYBER_ILLEGAL_SLANG	Slang used in cybercriminal context
MILITARY_SLANG	Slang used in military context

In the example text, the semantic engine detects ISIL as an abbreviation used in criminal and military context. Thus, it assigned a value of 3% for the criminal and military slang that is the result of dividing 1 between 31 distinct words appearing in the text excerpt (Table 17).

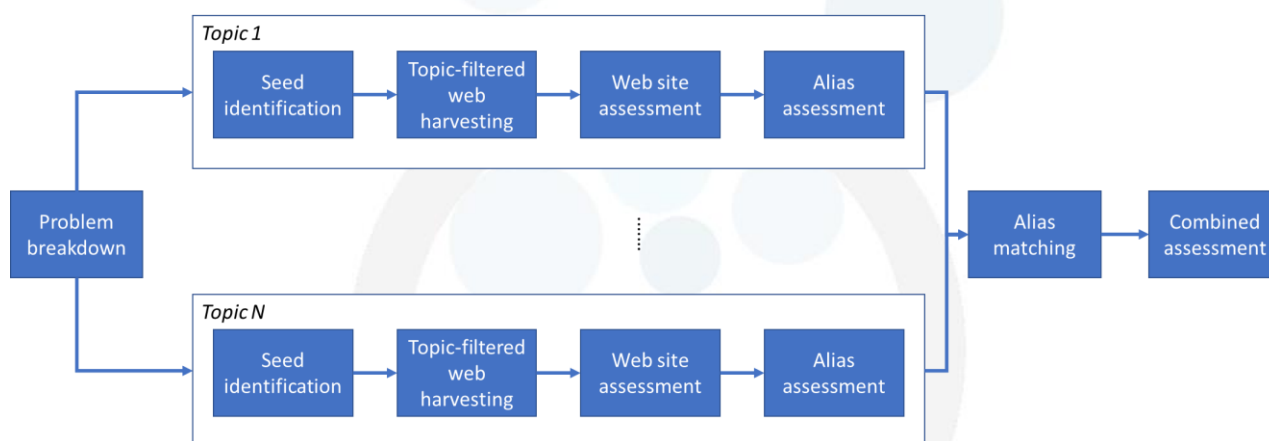
**Table 17 - Output of the intelligence engine**

Slang type	Percentage of slang use in the text
CRIMINAL_ENTERPRISE_SLANG	3%
MILITARY_SLANG	3%

### 7.2.3 Internet harvesting for lone wolf terrorist detection

As pointed out in Section 6.2.1, a lone wolf terrorist can pose serious threats to mass gathering events. The Swedish Defence Research Agency (FOI) has proposed a method (Brynielsson J., 2012) to analyse extremist forums to profile possible lone wolf terrorists looking for various digital traces, created when visiting extremist forums, making postings with offensive content, etc.

The proposed approach breakdowns the problem using the framework shown in Figure 7-2.



**Figure 7-2 - Lone wolf weak signal detection**

This approach could be considered by WP5, Task 5.3 to assess risks related to lone wolf terrorists.

## 7.3 HUMAN-CENTRED COMPUTER VISION

Useful weak signals that can be potentially acquired by computer vision tools, using existing methods, are the following:

- estimated crowd density;
- patterns of crowd movements (e.g., panic, increase in speed, group formation, drunkenness);
- specific individuals or groups moving in the scene;
- formation of groups of people exhibiting homogeneous clothing appearance;
- vehicles in the scene;
- abandoned objects.

A concise state-of-the-art is reported below of methods proposed in the computer vision academic literature for each of the above tasks.

### 7.3.1 Crowd density estimation

Crowd density estimation is one of the basic tasks addressed in the literature for crowd analysis. Density can be estimated from people counting, which however is accurate only for low-density crowds, or by analysing the crowd as a whole. Existing methods can be categorized into pixel-based, texture-based, and object-based (Silveira Jacques J.C., 2010). Pixel-based methods rely on local features (even extracted from individual pixels), obtained through background subtraction or edge detection. Texture-based methods use higher-level features computed from image patches (blocks of pixels). These two kinds of methods do not allow precise people counting and are therefore suitable only for density estimation. Object-based methods try to identify individuals in a scene instead, and provide people counting; therefore, in principle they also provide a more accurate density estimation. However, they are effective only in low-density crowds without severe occlusions; in dense crowds only density estimation is achievable, using pixel- or texture-based methods.

### 7.3.2 Patterns of crowd movements

Existing methods for detecting patterns of crowd movements can be categorized as bottom-up and top-down. Bottom-up methods are based on tracking individuals moving in a scene, and on the analysis of detected tracks to infer group or crowd behaviour; tracking individuals is however a difficult task in dense crowds. Top-down methods consider the crowd as a whole and analyse its global or local motion flow, e.g., based on the optical flow; this kind of method is not suitable for group detection. Methods for detecting patterns of crowd movement are also used to detect anomalous behaviours, usually defined as deviations from a model of normal behaviour (either predefined or learned from data). An example of top-down method for abnormal behaviour detection (defined as deviation from a normal model) is (Mehran R., 2009); in addition to optical flow it uses the social force model of pedestrian dynamics by (Helbing D., 1995), which has then been used in several subsequent works. Its accuracy depends mainly on crowd density; e.g., in experiments on low density crowd videos a true positive (TP) rate of 0.8 and a false positive (FP) rate below 0.1 are reported, whereas for high density crowds a TP rate of 0.8 was achieved at a FP rate around 0.4. Some top-down methods detect specific, medium-level patterns of movement, in contrast to high-level, semantic patterns like 'panic'. One example of such methods is the one by (Solmaz B., 2012), which detects bottlenecks, fountainheads, lanes, arches, and blocking patterns (see Fig. 1, top); as an interesting feature, it does not require object detection, tracking, nor training; on real video sequences with high crowd density, a TP rate of 0.8 was reported by the authors, with a FP rate around 0.05 to 0.2, depending on the specific pattern of movement. Another example is the method by (S. Wu, 2017), which detects lane, clockwise arch, counter-clockwise arch, bottleneck and fountainhead patterns (see Figure 7-3, bottom), with a similar performance as (Solmaz B., 2012) (the software implementation by the authors is available).

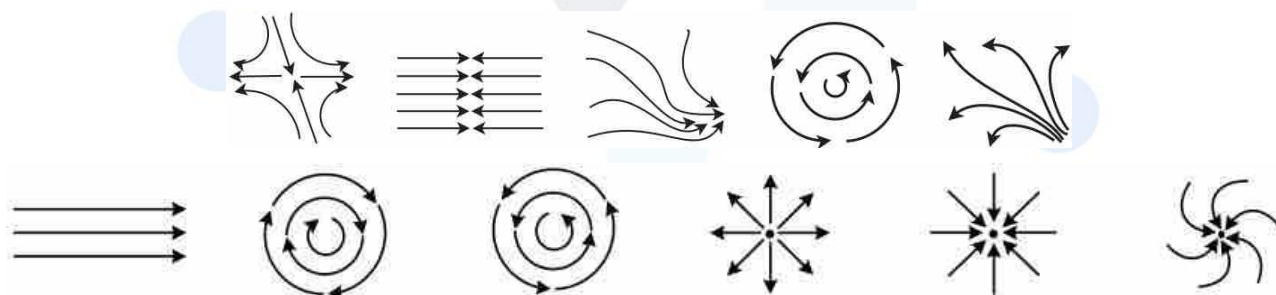


Figure 7-3 - The patterns of crowd movements

With regard to the specific task of detecting group formation, this is a challenging problem, also because it requires accurate detection and tracking of individuals. It is less studied than other crowd analysis tasks (Ge W., 2012), and only recently some promising results have been achieved (Solera F., 2016). The main existing methods focus on low-density crowd scenarios and exploit sociological models of human collective behaviour (Ge W., 2012) (Solera F., 2016). One issue is that no agreed performance (accuracy) metric exists for this kind of computer vision task (Solera F., 2016).

### **7.3.3 Specific individuals or groups moving in the scene.**

Tracking individuals is a well-known and widely studied computer vision tasks and is an instance of the more general object tracking task. It can be carried out accurately on low-density crowds. Recent works have addressed the tracking problem also in dense crowds, for instance (Idrees H., 2014). A useful reference for the specific task of online tracking of a single individual (object), starting from a bounding box provided as input and without pre-training, is the experimental analysis of state-of-the-art object tracking methods in (A.W.M. Smeulders, 2014).

Group tracking is a distinct problem instead, for which no significant, specific works exist. In principle, methods based on group detection (which in turn require individual tracking) could be used, like the ones mentioned above.

### **7.3.4 Formation of groups of people exhibiting homogeneous clothing appearance.**

This is a very specific kind of crowd-related event, for which no specific method exists. In principle, this event can be detected by combining group formation detection (discussed above) with the analysis of clothing appearance, which can be carried out through the same methods used for person re-identification (by comparing the clothing appearance of individuals in the detected group, either among themselves or with an image provided by the operator) or for people search (matching the clothing appearance of individuals to a given description). This implies that accurate detection can be achieved only for low-density crowds.

### **7.3.5 Detection and behaviour analysis of vehicles in the scene.**

The kind of weak signal in this case can be, e.g., the detection of a vehicle parked in a suspect location, or of a moving vehicle which may be used as a weapon. This can be achieved through object detection and tracking techniques, possibly tailored to vehicles, possibly combined with context information (e.g., definition of restricted access areas or sensitive areas in the camera field of view) to trigger alarms. Existing methods for vehicle detection and tracking are focused on traffic monitoring, e.g. (Rios-Cabrera R., 2012) (Sivaranam S., 2013), and their effectiveness to scenarios of interest to LETSCROWD has to be verified (for instance, the kind of occlusion in images of a crowd is likely to be different than in a traffic monitoring setting).

### **7.3.6 Detection of abandoned objects**

Detection of abandoned objects (e.g. luggage and backpacks) is a challenging computer vision task, as it requires a high-level understanding of a scene. Several methods have been proposed in the literature, and a few data sets are also available for experimental evaluations (Ferryman J., 2013) (Tian Y., 2011). They are focused on relatively simple scenarios with a low-density crowd. Notably, the method in (Ferryman J., 2013) was developed in the context of the EU project SUBITO (Surveillance of Unattended Baggage and the Identification and Tracking of the Owner), funded under the FP7-SECURITY Programme<sup>21</sup>.

---

<sup>21</sup> <http://www.subito-project.eu>



## 7.4 HUMAN AS SENSOR

A person present at the event is quite often the most reliable source of information to be used as precursor of security threats.

The main difference on the reliability of the collected information is the level of training received by the individual concerned:

- **Policemen** that have obviously a high level of training and are the best suited to detect precursors with high reliability as soon as they manifest. However, the number of policemen that can be deployed at events venue is normally limited.
- **Stewards** are normally organiser's employee whose level of training depends on many factors (national legislation, attitude of the employer, education, etc.). There are emerging standards on how to train stewards when dealing with mass gatherings such as the SKASS22 (SkillsActive, 2015) recently published by the National Occupational Standards<sup>22</sup> in UK, but they are not yet widely adopted so the level of reliability of stewards may vary across Europe.
- Simple participants to the event are usually not security trained and are subject to highly-possible misunderstandings (e.g. shouting and train noises mistaken for terrorist attacks on Madrid and Barcelona metro<sup>23</sup>) or the bystander effect. This is why the feedback received from the crowd is filtered by LEAs through either call centres or internet forms (an example is the form shown in Figure 7-4. used by UK Metropolitan Police<sup>24</sup>)

<sup>22</sup> <https://www.ukstandards.org.uk>

<sup>23</sup> <https://www.thinkspain.com/news-spain/27949/shouting-and-train-noises-mistaken-for-terrorist-attacks-on-madrid-and-barcelona-metro>

<sup>24</sup> <https://www.met.police.uk/tell-us-about/possible-terrorist-activity/report-possible-terrorist-activity/>



## About the suspicious activity

Even if you're not 100% sure, or it seems trivial, please provide as much information as you can so that our specially trained officers can look into it.

Who is, or was, involved?

☐ I don't know

Where did this happen?

☐ I don't know

When did this happen?



If you don't know or remember the exact date, please describe additional details that will help us to identify the date or time

Please tell us everything you can about what you've seen or heard and why it raised your suspicion.\*

Figure 7-4 - The UK Metropolitan Police suspicious activity report form

## 7.5 RELATIONSHIPS BETWEEN WEAK SIGNALS AND MASS GATHERING THREATS

### 7.5.1 Relationship between weak signals and threats' precursors

Some of the precursors of identified threats (Table 12 in Section 6.1) can be detected by the technologies for detecting weak signals described in the above Sections:

- Cyber Threat Intelligence (CTI)
- Human-Centred Computer Vision (HCCV)
- Semantic Intelligence (SI)
- Human as Sensor (HS)

The following represents a summary of the potential detection capability of each technology versus each identified precursor with a qualitative indication of its detection potential using a 3 levels' scale: Low (L), Medium (M) and High (H).

It is important to note that the advantage of the identified technologies vs. the human is that they can work 24/24 hours 7/7 days, so when evaluating the detection/sensing capabilities this has to be taken into account.

**Table 18 - Threat's precursor detection**

Threat precursor	LETSCROWD technology	Detection capability
Filming, taking notes or photographs, or watching for extended periods, focusing on security cameras, hallways, fire exits, access and egress routes	CTI	-
	HCCV	L/M
	SI	-
	HS	H
People behaving strangely, e.g. nervous, perspiring, wearing overly warm clothing, concealing their face, repeatedly patting upper body parts, etc.	CTI	-
	HCCV	L/M
	SI	-
	HS	-
People bringing unusual packages into your event (e.g. a disproportionate weight of luggage considering its size)	CTI	-
	HCCV	L
	SI	-
	HS	H
People found in off limits areas, particularly near plant or server rooms or places of concealment	CTI	-
	HCCV	H
	SI	-
	HS	M
Vehicles parked in suspicious circumstances	CTI	-
	HCCV	H
	SI	-
	HS	M
Anomalous vehicle e.g. a vehicle with different front & back license plates, with apparent heavy weight on rear axle, with large containers or gas containers inside, with additional visible improvised electrical wires	CTI	-
	HCCV	H
	SI	-
	HS	L/M
Anyone buying or storing a large amount of chemicals, fertilisers or gas cylinders for no obvious reasons	CTI	L
	HCCV	-
	SI	-
	HS	-
Social network activities	CTI	H
	HCCV	-
	SI	M/H
	HS	-
Splitting into groups (signalling multiple points of attack)	CTI	-
	HCCV	M
	SI	-
	HS	L
Identical luggage carried by several persons	CTI	-
	HCCV	M
	SI	-
	HS	L
Abandoned object	CTI	-

Threat precursor	LETSCROWD technology	Detection capability
	HCCV	M
	SI	-
	HS	H
Cyber-attack to critical infrastructures	CTI	
	HCCV	
	SI	
	HS	
	CTI	M
	HCCV	-
Signs of radicalisation on social media	SI	M
	HS	-
	CTI	-
Group of many persons with similar symbols (clothing, flags, etc.)	HCCV	M
	SI	-
	HS	M
	CTI	M
	HCCV	-
	SI	H
Mobilisation via social media	HS	-

Table 18 can be the basis for the labelling of each received weak signal according to its trustability to improve risk aware decisions to the stakeholders involved in the management of a mass gathering event.

Table 18 will be updated following another iteration with the LEAs involved in the project and will be reported in Deliverable D3.4.

### 7.5.2 Weak signals interpretation

As already discussed in the previous sections, weak signals or threat indicators may be received from various sources throughout the various stages of mass gathering event risk assessment. Those sources may include:

- Intelligence information
- Police reports
- Observations & reports from LEA's personnel, stewards and public
- Security systems

The threat level associated with weak signals may include, for example, the following levels:

Level	Definition
Low	General information about adversary intentions
Medium	Specific information regarding capabilities, planning and preparations, initial reports about suspicious activity at the target or its vicinity
High	Focused, credible information regarding actual preparations to mount attack, supporting evidence, indications to dry runs and collection of information

An example on how weak signals could be interpreted by an operator supported by a situational awareness tool is shown in Table 19 with the escalation of the level of risk on the basis of the reliability of the source of information.

**Table 19 – Example of a sequence of correlated weak signals**

Weak signal	Info source	Associated threat level
Jihadists web sites encourage supporters to attack targets in the country	SI	Low
Communication in dark web between jihad activists about possible action against the event	CTI	Low
Jihad activists search internet for instruction in bomb making and dual use materials	CTI	Medium
Police report about break-in to storage site and theft of large quantity of fertilizers	Police	Low
CCTV footage of event site show two persons loitering and taking pictures	HCCV	Medium
Security officer report during the event observation about two persons carrying identical bags avoiding security personnel and splitting	HS	Medium
Report from public about abounded bag found hidden under bench	HS	High

## 8 WAY FORWARD IN LETSCROWD AND CONCLUSIONS

### 8.1 IMPLEMENTATION OF A PRACTICAL APPROACH

From the analysis of the problem in the previous sections it is possible to draw the following conclusion that will be the basis for the implementation of a practical approach:

- The main threats of interest for LETSCROWD are those linked to terrorism including lone wolves and domestic extremisms, since the risks associated to clashes between different groups are already well known by LEAs and much more predictable in terms of dynamic behaviour.
- Given the above assumption, most of the risks to be considered are falling within the Low Probability High Impact category, thus making difficult to collect data on likelihoods and consequences.
- The Static Risk Assessment phase of the involved LEAs appears to be well structured according to standard principles of risk assessment and therefore it can be simply improved by introducing:
  - Crowd modelling to better assess consequences on participants;
  - Data analytics to improve the extraction of knowledge from databases of past events.
- The difficulty in collecting statistical evidence on the most critical threats makes the qualitative approaches more appropriate for the LETSCROWD Dynamic Risk Assessment, taking also into account the need to have the “man in the loop”.
- The most promising approach appears to be a situational awareness tool integrating:
  - Real-time GIS able to manage heterogeneous alerts.
  - A standardised protocol to handle risk-related geo- and time-referenced alerts.
  - A semi-automatic procedure to
    - Manage the alerts and evaluate how they dynamically contribute to the risk(s) for which they can be considered precursors.
    - To display the most significant alerts to the operator to allow him to dynamically modify the levels of the different considered risks accordingly;
    - Identify and show to the operator the most appropriate procedures to handle the new levels of risk.

### 8.2 CONCLUSIONS

The analysis carried out and reported in this document has allowed the identification of the most appropriate way forward to implement a Dynamic Risk Assessment methodology for mass gathering events in support to LEAs risk aware decision making.

The findings of this document will form the starting point for the coming WP3 deliverables:

- D3.3 Progress report on soft and hard mitigations.
- D3.4 LETSCROWD ESM implementation guidelines for crowd protection Version 1

## 9 REFERENCES AND ACRONYMS

### 9.1 REFERENCES

- A.W.M. Smeulders, D. C. (2014). Visual Tracking: An Experimental Survey. *IEEE Trans. on Pattern Analysis And Machine Intelligence*, 36(7), 1442-1468.
- Allen, R. (2012). HPA approach to dynamic risk assessment. *Presentation at SBSO@CRUK Cambridge*.
- Ben-Gal, I. (2007). Bayesian Networks. In R. K. F. Ruggeri, *Encyclopedia of statistics in quality and reliability*. John Wiley & Sons, Ltd.
- Bindner, L. (2017). *The Fight Against Online Jihadist Content*. Paris: MILIPOL Fair.
- Bladon P., H. R. (2002). Situation assessment using graphical models. *Proceedings of the Fifth International Conference on Information Fusion*. Annapolis, MD, USA.
- Brynielsson J., H. A. (2012). Analysis of Weak Signals for Detecting Lone Wolf Terrorists. *2012 IEEE European Intelligence and Security Informatics Conference*.
- Cambridge University Press. (n.d.). Retrieved from Cambridge Dictionary: <https://dictionary.cambridge.org/dictionary/english/security>
- Chakir E., M. M. (2017). A Real-Time Risk Assessment Model for Intrusion Detection Systems. *2017 IEEE International Symposium on Networks, Computers and Communications (ISNCC)*.
- Cohen K., J. F. (2014). Detecting Linguistic Markers for Radical Violence in Social Media. *Terrorism and Political Violence*, 26, 246–256.
- Coppola, D. P. (2006). *Introduction to International Disaster Management*. Elsevier.
- Council of the European Union. (2010). Internal security strategy for the European Union - Towards a European Security Model. General Secretariat of the European Council.
- Endsley M.R. (1995). Towards a theory of situation awareness in dynamic systems. *Human Factors*, 37(1), 32-64.
- European Commission. (2017). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Eleventh progress report towards an effective and genuine Security Union.
- Ezell B.C., B. S. (2010). Probabilistic Risk Analysis and Terrorism Risk. *Risk Analysis*, 30(4). doi:10.1111/j.1539-6924.2010.01401.x
- Federal Emergency Management Agency (FEMA). (2005). *Risk Assessment - A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*.
- Ferryman J., H. D.-S. (2013). Robust abandoned object detection integrating wide area visual surveillance and social context. *Pattern Recognition Letters*(34), 789-798.
- Fredholm, M. (2011). Hunting Lone Wolves – Finding Islamist Lone Actors Before They Strike. *Stockholm Seminar on Lone Wolf Terrorism*.
- Ge W., C. R. (2012). Vision-Based Analysis of Small Groups in Pedestrian Crowds. *IEEE Trans. Pattern Anal. Mach. Intell.*, 34(5), 1003-1016.
- Haimes, Y. (1988). *Risk modelling assessment and management*. John Willey & Sons.
- Helbing D., M. P. (1995). Social force model for pedestrian dynamics. *Physical Review E*, 51(5).
- Hope, B. (2004). Using Fault Tree Analysis to Assess Bioterrorist Risks to the U.S. Food Supply. *Human and Ecological Risk Assessment*, 10(3).
- Hossen K., S. Z. (2013). *Applying Fuzzy Logic to Risk Assessment and Decision-Making*. Casualty



Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries.

- Idrees H., W. N. (2014). Tracking in dense crowds using prominence and neighborhood motion concurrence. *Image and Vision Computing*, 32, 14-26.
- International Organization for Standardization . (2009). IEC/ISO 31010 Risk management – Risk assessment techniques.
- International Organization for Standardization. (2009). ISO 31000 Risk management — Principles and guidelines.
- Jha, M. K. (2009). Dynamic Bayesian Network for Predicting the Likelihood of a Terrorist Attack at Critical Transportation Infrastructure Facilities. 15(1).
- Kollek D. (2014). *An Introduction to Mass Gatherings*. Centre for Excellence in Emergency Preparedness.
- LETS-CROWD project. (2017). *Deliverable D2.2 LETSCROWD Use Cases, Scenarios and KPIs identification*.
- Linwood D. Hudson, B. S. (2005). An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners.
- Mehran R., O. O. (2009). Abnormal Crowd Behavior Detection using Social Force Model. *CVPR*.
- Meloy J.R., H. J. (2012). The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology. *Behavioural Science and the Law*, 30(3).
- Nima Khakzad, F. K. (2014). Risk Management of Domino Effects Considering Dynamic Consequence Analysis. *Risk Analysis*, 34(6).
- OASIS Consortium. (2010). *Common Alerting Protocol Version 1.2*.
- Paul J.H. Schoemaker, G. S. (2009). How to Make Sense of Weak Signals. *MIT Sloan Management Review*, 50(3).
- Peterson J., D. J. (2017, 8 23). *How social media sends extremism into overdrive*. Retrieved from CNN: <https://edition.cnn.com/2017/08/23/opinions/social-media-fuels-right-wing-extremism-opinion-peterson-densley/index.html>
- Pramanik M.I., L. R. (2017). Big data analytics for security and criminal investigations. *WIREs Data Mining and Knowledge Discovery*.
- Raineri, A. S. (2015). *Behavioural risk at outdoor music festivals*. Doctoral Thesis, University of Southern Queensland.
- Rios-Cabrera R., T. T. (2012). Efficient multi-camera vehicle detection, tracking, and identification in a tunnel surveillance application. *Computer Vision and Image Understanding*, 116, 742-753.
- S. Alava, D. F.-M. (2017). *Youth and violent extremism on social media: mapping the research*. UNESCO - United Nations Educational, Scientific and Cultural Organization.
- S. Wu, H. Y.-H. (2017). Crowd Behavior Analysis via Curl and Divergence of Motion Trajectories. *Int. J. Computer Vision*, 123, 499–519.
- Sageman, M. (2008). *Leaderless Jihad: Terror Networks in the Twenty-First Century*. University of Pennsylvania Press.
- Semenov A., V. J. (2010). Analysing the presence of school-shooting related communities at social media sites. *Int. J. of Multimedia Intelligence and Security*, 1(3).
- Silveira Jacques J.C., M. S. (2010). Crowd analysis using computer vision techniques. *IEEE Signal Process. Mag.*, 27(5), 66–77.
- Sivaranam S., T. M. (2013). Looking at Vehicles on the Road: A Survey of Vision-Based Vehicle Detection Tracking and Behavior Analysis. *IEEE Transactions on Intelligent Transportation Systems*, 14(4), 1773-1795.

- SkillsActive. (2015). *Control the movement of spectators and deal with crowd issues at an event*. National Occupational Standards.
- Solera F., C. S. (2016). Socially Constrained Structural Learning for Groups Detection in Crowd. *IEEE Trans. Pattern Anal. Mach. Intell.*, 38(5), 995-1008.
- Solmaz B., M. B. (2012). Identifying Behaviors in Crowd Scenes Using Stability Analysis for Dynamical Systems. *IEEE Trans. Pattern Anal. Mach. Intell.*, 34(10), 2064-2070 .
- Spaaij R. (2010). The Enigma of LoneWolf Terrorism: An Assessment. *Studies in Conflict & Terrorism*, 33(9).
- Stratton, S. J. (2013). Violent Sabotage of Mass-Gathering Events. *Prehospital and Disaster Medicine*, 28(4).
- Tian Y., F. R. (2011). Robust Detection of Abandoned and Removed Objects in Complex Surveillance Videos. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 41(5), 565-576.
- UK Government Office for Science. (2011). *Blackett Review of High Impact Low Probability Risks*.
- UK Health and Safety Executive. (2000). *Managing crowds safely - A guide for organisers at events and venues*.
- Vose, D. (2000). *Risk Analysis*. John Wiley & Sons Ltd.
- Waters D. (2011). *Quantitative Methods for Business*. Pearson.
- Wierman M.J. (2010). *An Introduction to the Mathematics of Uncertainty: including Set Theory, Logic, Probability, Fuzzy Sets, Rough Sets, and Evidence Theory*. Creighton University. Retrieved from [https://www.creighton.edu/fileadmin/user/CCAS/programs/fuzzy\\_math/docs/MOU.pdf](https://www.creighton.edu/fileadmin/user/CCAS/programs/fuzzy_math/docs/MOU.pdf)
- Willis H.H., M. A. (2005). *Estimating Terrorism Risk*. RAND Corporation - Center for Terrorism Risk Management Policy.
- Woodhouse, P. (2018, February 1). *Preventing vehicle ramming attacks in the age of driverless cars*. Retrieved from IFSEC Global: <https://www.ifsecglobal.com/preventing-vehicle-ramming-attacks-age-driverless-cars/>
- World Health Organisation (WHO). (2008). *Communicable disease alert and response for mass gatherings: key considerations*.
- World Health Organisation (WHO). (2015). *Public health for mass gatherings: key considerations*.

## 9.2 ACRONYMS

Acronym	Definition
AI	Artificial Intelligence
ALARA	As Low As Reasonably Achievable
ALARP	As Low As Reasonably Possible (or Practicable)
APT	Advanced Persistent Threat
BN	Bayesian Network
CAP	Common Alerting Protocol
CBA	Cost Benefit Analysis
CBRN	Chemical, Biological, Radiological and Nuclear
CCTV	Closed-Circuit Television
COTS	Commercial Off The Shelf
COTS	Component-Off-The-Shelf
CTI	Cyber-Threat Intelligence
CTI	Cyber Threats Intelligence
CVE	Common Vulnerability Exposure
DRA	Dynamic Risk Assessment
ESM	European Security Model
ETA	Euskadi Ta Askatasuna
FMEA	Failure Mode and Effect Analysis
FP	False Positive
FTA	Fault Tree Analysis
GIS	Geographic Information System
GTD	Global Terrorism Database
H	High
HAZOP	Hazard and operability
HCCV	Human-Centred Computer Vision
HS	Human as Sensor
HUMINT	Human Intelligence
IDS	Intrusion Detection System
IED	Improvised Explosive Device
IOA	Indicators of Attack
IOC	Indicators of Compromise
IoT	Internet of Things
IPTC	International Press Telecommunications Council

Acronym	Definition
IRA	Irish Republican Army
ISIL	Islamic State of Iraq and the Levant
ISO	International Standardisation Organisation
L	Low
LEA	Law Enforcement Agency
M	Medium
OASIS	Organization for the Advancement of Structured Information Standards
OSINT	Open Source Intelligence
PDF	Probability Density Function
PDT	Probabilistic Decision Tree
PFD	Process Flow Diagram
PSA	Probabilistic System Assessment
RAT	Remote Access Trojan
SI	Semantic Intelligence
SMI	See SOCMINT
SOCMINT	Social Media Intelligence
SRA	Static Risk Assessment
STIX	Structured Threat Information Expression
SW	Software
TAXXI	Trusted Automated Exchange of Intelligence Information
TINT	Technical Intelligence
TP	True Positive
UEFA	
UNESCO	United Nations Educational, Scientific and Cultural Organization
USA	United States of America

## 10 APPENDIX 1 - EXAMPLE OF A SECURITY EVENT IN GERMANY

### 10.1 POLICE AND EVENTS

Ensuring public order and safety in the context of events requires intensive cooperation between the police, the organiser, the competent licensing authorities as well as the security authorities and organisations (BOS) of non-police risk prevention.

The primary objective of the police regarding the management of major events is to ensure that the event takes place in full security. Accordingly, relevant concepts include both preventive and repressive measures.

### 10.2 TASKS

The tasks of the police in the context of event management, irrespective of the phase of the event, derive from the respective police acts of the states as well as the federal government, and are specified by appropriate regulations (e.g. "Polizeidienstvorschrift 100"). In particular, the core tasks include:

- Risk prevention
- Prosecution of criminal and administrative offences
- Administrative assistance and enforcement aid

In general, it is the organizer's responsibility, if necessary together with his security service, to provide venue safety and security. The police support at best in certain aspects and only if necessary.

### 10.3 DESCRIPTION OF POLICE ACTIVITIES

#### 10.3.1 Before the event: Preparation

It is essential that the police obtain information of a planned event as early as possible. In this regard, appropriate measures may include, for example, specified information sharing with licensing authorities, internet research, social media etc.

Another important aspect is the close collaboration with the organiser and other relevant actors (e.g. municipality, fire brigade, rescue service), even during the preparatory stage.

The police participate in the voting rounds or coordination groups in an advisory capacity and is, if necessary, available for bilateral agreements. The police is particularly involved in the preparation and examination of the security concept, which must be developed in accordance with the requirements of the respective state law and in coordination with the competent police authority.

As part of joint on-site inspections, the police also participate in the formal acceptance of the event site and verifies the implementation of security agreements and official requirements.

#### 10.3.2 During the event: Implementation

The stage of operation at events is subdivided in arrival, event and departure.

The police is generally responsible for defense and the prosecution of criminal offences. Taking into account the responsibilities, resources and competencies of other actors, the police will cover the duties of others only if they are unable to take action or unable to take timely action. In an emergency situation, the police support the crisis management via its involvement in the crisis management structures (setting up of a crisis unit etc.).

### 10.3.3 Follow-up

Systematic review and evaluation of operation: The police review its concepts in terms of achieving the objectives in order to gain new insights for the planning and implementation of forthcoming events. Special emphasis is on the organisation of collaboration with relevant non-policing actors.

## 10.4 RISK ASSESSMENT

Risk assessment represents a fundamental aspect in preparation for the operation. It forms the basis for a scenario description, the development of a security concept as well as the planning of forces.

The hazards and risks in the context of major events (in differentiation from those of everyday life):

- Mass phenomena (e.g. panic reactions)
- High concentration of people with social, medical, physical and technical implications
- Risk of crime and threat of terrorism

The evaluation process considers the factors potential extent of damage and likelihood of occurrence.

If all threats are evaluated, prioritized and summarized (e.g. in form of a risk matrix) with regard to their potential of endangering relevant protection objectives, the police will verify the feasibility of a safe event.

- Potentially classified threats should be reduced to an acceptable level by means of appropriate security measures.
- The achievement of objectives should be determined by mutual agreement of all parties involved.

## 10.5 ROLE OF THE POLICE IN THE LICENSING PROCEDURE

### 10.5.1 Objectives

As part of the preparation and risk assessment, the responsible police department is involved in the official approval procedure. The aim of the police should be to influence the planning and implementation that security risks are excluded or minimized by means of appropriate measures on the part of the organiser.

The police can check and verify at an early stage what measures are necessary for a safe event and obtain the relevant specifications or agreements.

### 10.5.2 Legal grounds for police involvement

§29 (2) StVO in conjunction with the relevant administrative regulation provide that the police must be consulted for the approval procedure of major events. The same applies to events in places of assembly on the basis of §43 (2) sentence 1 MVStättVO (Muster-Versammlungsstättenverordnung).

In some federal states, the procedural involvement of the police in the authorization procedure of events is also governed by state law. For example, in Bavaria, § 19 VollzBekLStVG provides that the competent authorities have to verify whether permission is to be refused to prevent threats or significant disadvantages / nuisances for the general public or neighborhood, or to prevent significant impairments of nature and landscape.

It should be noted, however, that the system of consultation is not legally binding but left to the discretion of the competent authority.

### 10.5.3 Factors for successful police involvement

The main factors for successful police involvement are:

- Early involvement



- Standardized responsibilities
- Permanent contacts at local level
- Integration into the decision-making processes related to safety
- Continuous coordination processes
- Approval after the submission of all statements and suggestions for improvement

#### **10.5.4 Organizational structure of the police during an event**

##### **10.5.4.1 General and specific structure**

Due to the complexity of the situation, events are usually not addressed through the General Organisational Structure (Allgemeine Aufbauorganisation AAO) but rather through an adapted Specific Organisational Structure (BAO). The BAO is organized hierarchically and takes into account the interfaces with relevant non-police actors as well as other specific structures (coordination group, crisis unit).

##### **10.5.4.2 Outline of the specific organizational structure**

If it is expected that the event requires extensive measures, it is frequent practice to form operational sections (EA).

Example of a useful structure for an event:

- Information: Observation of people on and off-site and early identification of potential hazards
- Protection: Prevention through presence on the event-site, its surroundings and access roads. Investigation measures in case of criminal offenses.
- Traffic measures (in case of a large number of visitors).
- Criminal prosecution (insults, theft, personal injury, etc.)
- Central services: technology and supply

##### **10.5.4.3 Police measures during an event**

Although not originally responsible for events, the police implement numerous measures in the context of events depending on the requirements:

- Internal and external documentation of deployment
- Patrols and controls
- Investigation and high presence
- Measures to protect minors (alcohol consumption)
- Material and personal support of the organiser in case of cancellation or evacuation

#### **10.6 PRESS AND PUBLIC RELATIONS**

The police should be involved in the planning of the media infrastructure at events with a high media attendance. Close consultation is also recommended for actual press and public relations. Clear procedures and distribution of roles facilitate actions for all parties concerned.

For major events it is useful to establish media focal points

Crisis communication:

- Any information provided by the police must be verified in advance.
- Participants and third parties should be continuously informed about the crisis situation.

- Official problem statements are essential for the credibility: the police always reserves the right to intervene within the scope of their legal mandate.

