Title:	Document Version:
D3.6 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*:
M20 (31 December 2018)	7 January 2019	R-PU

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

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

Responsible:	Organisation:	Contributing WP:
Carlo Dambra	ZB	WP3

Authors (organisation):

C. Dambra (ZB), C. Graf (RAILSEC), Y. Alon (RAILSEC), 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), M. Bolognesi, G. Garzo, A. Antinori (INTERNO), G. Fumera (UNICA), D. Ariu (PLURIBUS)

Abstract:

This document represents a revised version of Deliverable D3.2 and D3.4 including:

- An updated summary of the findings of Deliverable D3.2 on vulnerabilities, threats and hazards, the related likelihoods and consequences.
- An improved version of the Dynamic Risk Assessment (DRA) methodology after a series of interactions with the involved LEAs.
- The most innovative contributions on
    - The analysis of the credibility and reliability of the sensors used to detect weak signals.
    - The rules to be applied for the clustering of Weak Signals into Suspicious Events or Patterns.

Keywords:

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

Revision History

Revision	Date	Description	Author (Organisation)
V0.00	12.11.2018	Table of Content	C. Dambra (ZB)
V0.01	10.12.2018	First draft	C. Dambra (ZB)
V0.02	14.12.2018	First round of partners contributions	See authors in cover page
V0.03	19.12.2018	Second round of partners contributions	See authors in cover page
V0.04	28.12.2018	Final version ready for review	C. Dambra (ZB)
V1.00	07.01.2019	Final version ready for submission after review from DBLUE and CROWD.	C. Dambra (ZB)

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

More information available at https://letscrowd.eu

Copyright Statement

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

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

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

Executive Summary

This document represents a revised version of Deliverable D3.2 and D3.4 including:

- An updated summary of the findings of Deliverable D3.2 on vulnerabilities, threats and hazards, the related likelihoods and consequences for crowds during mass gathering events.
- An improved version of the Dynamic Risk Assessment (DRA) methodology after a series of interactions with the involved LEAs.
- The most innovative contributions on
  - The analysis of the credibility and reliability of the sensors used to detect weak signals.
  - The rules to be applied for the clustering of Weak Signals into Suspicious Events or Patterns.

The analysis of the sensors used to detect weak signals focuses on the evaluation of the reliability of each technology developed/improved in LETSCROWD (Human-Centred Computer Vision, semantic intelligence and web crawler) in detecting Weak Signals corresponding to specific threat precursors and on the reliability of different categories of human as a sensors in reporting suspicious behaviours: highly-trained police forces, basic-trained police forces, stewards and citizens.

The document then reports a series of rules, validated by the LEAs involved in the DRA, to increase the situational awareness of a LEA operator managing a crowded event. These rules are centred around the identification of possible simultaneous (in space and/or time) weak signals potentially interpretable as threat precursors (e.g. possible diversions like putting fire to garbage collectors on the road or simultaneous road accidents close to the event venue, simultaneous suspicious behaviours of some individuals, suspicious cyber-attacks to organisations that – after some time – become involved in the event organisation, etc.).

Finally, the scenarios defined for the implementation of the Practical Demonstrations of the DRA for the involved LEAs are reported:

- Ertzaintza (ERT) in Bilbao based on the Holy Weeks processions (18-22 April 2019).
- Ayuntamiento de Madrid (AdM), based on the LGBTIQ (lesbian, gay, bisexual, transgender, intersex and queer) Pride week on early July 2019.
- Hochschule für den öffentlichen Dienst in Bayern (BayFHVR), simulating a visit of the Ministry of the Interior at the school.

Index

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 PURPOSE OF THE DOCUMENT

As described in the DoA, this report will identify vulnerabilities, threats and hazards, the related likelihoods and consequences for crowds during mass gathering events.

1.2 SCOPE OF THE DOCUMENT

The scope of this document is to summarise the findings of its predecessors, Deliverables D3.2 and D3.4, on vulnerabilities, threats and hazards, the related likelihoods and consequences and to update them with the information gathered from the LEAs during several face-to-face meeting on

- The reliability of the sensors to be used in the DRA (including the human as a sensor);
- On how to cluster weak signals using pre-defined rules;
- The scenarios to be implemented at LEAs premises to demonstrate the usefulness of DRA.

1.3 STRUCTURE OF THE DOCUMENT

The document is structured as follows:

- Section 2 summarises the findings on vulnerabilities, threats and hazards, the related likelihoods and consequences described in Deliverables D3.2 and D3.4 (its predecessors) to help the reader in understanding the whole approach;
- Section 3 describes the Dynamic Risk Assessment (DRA) that has been revised after interaction with the LEAs involved;
- Section 4 proposes a discussion on the credibility and reliability of sensors to be used in the detection of Weak Signals (WS);
- Section 5 lists a first set of rules to be applied to support the operator to cluster WS into Suspicious Events or Patterns.
- Section 6 introduces the scenarios to be used to implement the Practical Demonstrations of the DRA at LEAs premises.
- Finally, Section 7 proposes the way forward and the conclusions that can be drawn from the document.

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)	The Dynamic Risk Assessment is defined by the Health Protection Agency (HPA)[1] in UK as the "*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*".

[1] http://www.istr.org.uk/docs/dymamicriskassessment.pdf

Term	Definition
	In LETSCROWD the **Dynamic Risk Assessment** definition can be modified as follows: "*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*".
Hazard	Something that is dangerous and likely to cause damage.
Mass Gathering	A Mass Gathering event can be defined (1) as: "*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*".
Safety	Safety is defined in the Cambridge Dictionary (2) as "*a state in which or a place where you are safe and not in danger or at risk*".
Security	Security is defined in the Cambridge Dictionary (2) as "*Protection of a person, building, organization, or country against threats such as crime or attacks by foreign countries*". From a LEA prospective the definition of the word "security" implies, in addition to the above, also the activities of conservation of general public safety.
Situational Awareness	According to (3) "*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*".
Threat	An expression of intention to inflict evil, injury, or damage.
Weak Signal	A weak signal can be defined (4) as "*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*".

2 MAIN FINDINGS FROM DELIVERABLE D3.2

In this section a summary of Deliverable D3.2 is reported, to help the reader to understand the current approach. In particular:

1. The suggested way forward to implement the Dynamical Risk Assessment (DRA);
2. An example of the possible threat precursors to be identified by the weak signals detected by the identified sensors, the possible attack modes and, finally, the possible threats to the crowd.

2.1 IMPLEMENTATION OF A PRACTICAL APPROACH

From the analysis carried out in Deliverables D3.2 and D3.4 it is possible to draw the following conclusions forming the basis for the implementation of a practical approach for DRA:

- The main threats of interest for LETSCROWD are those linked to terrorism including so-called "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 fall within the Low Probability High Impact category, thus making difficult to collect data on likelihoods and consequences for crowds;
- 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;
        - 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;
        - Geo-reference the assets to be protected (places, objects, groups of people, etc.) and manage the variations in their vulnerability. That is to say, an asset that in principle has a very low vulnerability or is well protected and becomes vulnerable for different reasons or ceases to have protection.

2.2 SENSORS, PRECURSORS, ATTACK MODES AND THREATS

The sensors to detect threat precursors can be those listed in Table 2 (provided as example and not exhaustive, the list can be extended according to LEAs needs):

Table 2 - Possible sensor's types

Sensor ID	Sensor type	Description
S01	Cyber Threat Intelligence (CTI)	Detection of cyber-attack that can directly or indirectly compromise the security of the event, e.g. Distributed Denial of Service (DDoS) to the network supporting CCTV system.
S02	Human-Centred Computer Vision (HCCV)	Any camera-related system (fixed, mobile or drone-mounted) with the attached processing (including, e.g., face recognition, number plate recognition, motion detection, people tracking, 3D crowd fluxes based on stereo cameras, etc.).
S03	Semantic Intelligence (SI)	Detection of conversation on Open Sources or Social Networks that could represent a precursor of a threat.
S04	Human as Sensor (HS)	It can be a member of the public, a policeman, a member of the staff, someone from intelligence services or agencies etc. each one obviously with its own credibility.
S05	Physical Sensor (PS)	Mobile and/or wearable thermal sensors, explosive sensors, metal detectors, etc.

Each Weak Signal is related to - alone or in combination with other WSs - one or more **Precursors** (see examples in Table 3) of possible **Attack Modes** (Table 4) corresponding to possible **Threats to the crowd** (Table 5). These tables were already reported in Deliverable D3.4 and have been updated using partners' experience and available reports (5) (6).

Although the list of Precursors in Table 3 quite complete, it is important to always bear in mind that threats can be so, by a conjunction of details that can subjectively be interpreted as such when they are assessed within a given context, place, time, attitude and situation. Determining a generic and fixed list of threats' precursors limits other possible threats, so it is necessary to take into account other possible situations that together with others and under the human eye, may become a new threat. This aspect is therefore explicitly taken into account in the DRA methodology described in Section 3 when dealing with Suspicious Events and Patterns that can be generated either by automatic rules or by the man-in-the-loop identifying and correlating specific weak signals.

The Threat information is mainly used to set-up the event scenario (e.g. to a priori select the sources of information on which to crawl information knowing the expected threat) than to assess risk levels: when dealing with dynamic risk assessment is key to anticipate Attack Modes and the reason for the attack is less important.

Table 3 - Possible threat's precursors

Precursor ID	Precursor description
P01	Filming, taking notes or photographs, or watching for extended periods, focusing on security cameras, hallways, fire exits, access and egress routes
P02	People behaving strangely
P03	People bringing unusual packages into event
P04	People found in off limits areas, particularly near plant or server rooms or places of concealment

Precursor ID	Precursor description
P05	Vehicles parked in suspicious circumstances (e.g. vehicle parked near the venue, with one or more people remaining in the vehicle, for longer than would be considered usual)
P06	Anomalous vehicle
P07	Similar responses or suspicious activities (e.g., hoax devices or bomb threats) in multiple locations
P08	Suspicious social network activities (e.g. chat on social media that could be related to a possible attack to the crowd) or web content (e.g. a blog post urging to attack the crowd)
P09	Splitting into groups (signalling multiple points of attack)
P10	Identical luggage carried by several persons
P11	Abandoned object
P12	Cyber-attack to critical infrastructures
P13	Traceable signs of radicalisation on social media
P14	Group of people with similar symbols (clothing, flags, etc.)
P15	Mobilisation via social media
P16	Vehicle entering a pedestrian area
P17	Vehicle stolen
P18	Person collapsing
P19	People fighting
P20	High conjunction
P21	Crowd restricted movements
P22	Individual wearing clothing not suitable with the conditions of the location, time and weather
P23	Individual whose luggage is not compatible with his appearance
P24	Individual carrying a baggage that is disproportionately heavy to its dimension
P25	Individual showing nervousness or fear in front of police
P26	Individual showing interest for security, procedural and/or organisational aspects
P27	Two or more persons secretly keeping in touch
P28	Flying drone (or any other UAV)
P29	Pattern or series of false alarms indicating possible testing of security systems and observation of response behaviour and procedures (bomb threats, leaving hoax devices or packages)
P30	The same vehicle and different individuals or the same individuals in a different vehicle returning to a location(s)
P31	Delivery vehicles arriving at the event at the wrong time or outside of normal hours.
P32	Recent damage to perimeter security, breaches in fence lines or walls or the concealment in hides of mortar base plates or assault equipment
P33	Attempts to disguise identity - motorcycle helmets, hoodies, etc. or multiple sets of clothing to change appearance
P34	Extended wait in line for tickets or admission (can be a precursor for crowd control problems)
P35	Malicious acts requiring multiple responses with the need of specialized or technical equipment that reduces LEAs' resources allocated to the event.

Precursor ID	Precursor description
P36	A significant incident or several minor incidents that require a commitment of resources to investigate or mitigate
P37	Unusually high number of calls for service or incidence of activities inconsistent with typical patterns within the area of responsibility
P38	Burn marks or discoloration on walls, doors, ground, and/or floor; presence of unusual odors or liquids
P39	Unusual or unpleasant odours, chemical fires, brightly coloured stains, or corroded or rusted metal fixtures in otherwise dry and weather-protected environments
P40	Injuries or illness inconsistent with explanation
P41	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents [classified or unclassified]) that are proprietary to the facility

Table 4 - Possible Attack Modes

Attack Mode ID	Attack Mode description
AM01	(Squad of) Suicide bomber(s)
AM02	Vehicle used as weapon (vehicle ramming)
AM03	VBIED Vehicle-Born Improvised Explosive Device
AM04	Bomb/IED (e.g. in an abandoned object)
AM05	CBRN attack
AM06	Cold steel (e.g. stabbing)
AM07	Hijacking of social networks
AM08	Shooting
AM09	Combined attack (two or more attacks simultaneously launched against the event)
AM10	Riot
AM11	Fire
AM12	Drone-based attack
AM13	Hostages
AM14	Aircraft used as weapon
AM15	Sniper

Table 5 - Possible Threats to the crowd

Threat ID	Threat description
T01	Terrorism
T02	Domestic extremism
T03	Lone wolf
T04	Clashes between different groups
T05	Connected criminal activities

3 REVISED DRA APPROACH

3.1 WEAK SIGNAL (WS)

The Dynamic Risk Assessment (DRA) system bases its reasoning on the receipt and processing of **Weak Signal** (**WS**), the minimum quantum of information managed by the DRA.

Each Weak Signal generated by a sensor is sent to the control room for further processing embedded in a message containing the following minimal information:

- A unique **ID**;
- The absolute time **t** in which it has been generated;
- The **geolocation** (x, y) - if available;
- The signature of the detection, i.e. all the **features** related to what it has been detected by the sensor using a pre-defined semantic (e.g. using keywords);
- The **Reliability** (**R**) of the detection, e.g. a speeding car is detected with 95% reliability (where the expressed uncertainty could be generated by the difficulty in measuring the speed or by a tree shadowing the car);
- A **snapshot** of what has been detected to help the operator to confirm, discard (false alarm) or amend the detection of the sensor.

Each Weak Signal detected by Sensor m has a **Significance** (**S**) value assigned to it that is a combination of (see Section 4 for a more detailed discussion on reliability and credibility):

- The **Credibility** (**C**) of the Sensor m (assigned a priori by LEAs experts) in detecting the considered precursor;
- The **Reliability** (**R**) of the detection;
- The **Time Distance** (TD) from the event (a speeding car can be considered differently if it is happening 3 days before the event or during the event);

The Significance of the considered Weak Signal detected at time t by the Sensor m ranges in the [0, 1] interval and is computed as follows:

$$S(ID) = \frac{\alpha\, C(m) * \beta\, R(ID) * \gamma\, TD(t)}{Normalising\ Factor} \in [0,1]$$

where:

- C and R are typically integer between 1 and 5 (where 1 is very low and 5 is very high);
- TD is a value in [0, 1] depending if it is close or far from event (the closer the WS to the event execution the greater the TD value);
- The Normalising Factor keep S(ID) in [0, 1];
- α, β and γ are correcting factors to tune the role of each factor in the product.

As stated above, **Significance** assumes values in the [0, 1] interval, where 0 means **no significance** and 1 **maximum significance**.

3.2 SUSPICIOUS EVENTS AND PATTERNS

When a WS is received it is necessary to process it to evaluate if it can become, alone or in a group, of interest for the event. To this end two more structures are introduced:

- **Suspicious Event** (**SE**), build by a single WS that has sufficient significance to become an SE;
- **Suspicious Pattern** (**SP**), two or more WS can create a SP if they have sufficient significance and are linked together according to one of the criteria described below (see Section 3.2.2).

3.2.1 Suspicious Event

A WS can become a **Suspicious Event** (**SE**) per se according to its Significance and/or other conditions set in the system (e.g. the Sensor that has generated it, the specific detection that requires attention independently from the reliability of the detection, etc.). In this case, the Significance of the SE becomes the Significance of the WS:

$$S(SE) = S(ID)$$

Intelligence Alerts (**IA**), i.e. those signals coming from the intelligence services, can be considered a special Suspicious Event with maximum Significance S(IA) = 1.

3.2.2 Suspicious Pattern

A WS alone could be insignificant, but when put in combination with other WS could become important. Therefore, the WS could be grouped into a **Suspicious Pattern** (**SP**). To build a Suspicious Pattern at least 2 (two) WS are necessary.

The Suspicious Pattern can be generated:

1. Before the event takes place, using the **LEAs' knowledge** that defines the rules for building the patterns. The knowledge is specific to each LEA and mechanisms to share it according to existing EU/international protocols could be considered;
2. Dynamically, during event preparation and execution, using an automatic grouping of WS using logic similar to those currently used, for example, at some airport security checks: 3 or more credible WS (precursors) "**simultaneously**" (i.e. within a short period of time) coming from different sources of information can be considered as SP. The minimum number of credible WS can be adapted to the specific local conditions;
3. Dynamically, using **data analytics** that works on all received WS and generates suspicious pattern. There are more and more increasing concerns for intelligent systems to automatically discover unexpected behaviours or anomaly events from weak signals. Recently, researchers started to publish deep learning techniques to automatically learn high-level representations, and then avoid the requirement of domain experts in designing features (7) (8) (9).

Therefore, Suspicious Patterns can be of 7 types:

- **Group** (**GSP**): a set of WS (or SE or SP) without time and geographic constraints. The attention of the operator is raised when at least a subset of WS (or SE or SP) belonging to the pattern is received with a reasonable degree of significance. An example of a Group is the SP6 "Suspicious Vehicle" shown in Figure 1 with 4 WS attached to it representing the same truck detected by different sensors (details in Figure

2). It is sufficient to have received the WS independently of the time sequence in which they are detected to raise the attention of the operator;

- **Sequence** (**SSP**): a set of WS (or SE or SP) that need to be received in the correct sequence. An example of a Sequence is the Abandoned Object Pattern. It has 3 WS:

  1. Individual with a bag;
  2. Bag left unattended (from a steward);
  3. Individual leaving the scene for a given time (e.g. 10 minutes);

  It is necessary to detect the 3 precursors in the correct order to raise the attention of the operator. Another possible example is the following:

  1. Three individuals, e.g. wearing the same hat and carrying the same backpacks, arrive in the scene;
  2. One of them approaches a steward trying to gather information regarding the security systems and procedures;
  3. The 3 are separating to 3 different parts of the venue and disappear from the cameras;
  4. Backpack left unattended (from police);

- **Area** (**ASP**): a set of WS (or SE or SP) confined in the same area received in a pre-defined time interval. In this case the constrain is on being all within the same area;
- **Distance from Hot Spots** (DHSSP): a set of WS (or SE or SP) in a pre-defined time interval all at a distance from Hot Spots shorter than a given threshold (e.g. three events close to both the French and British consulates);
- **Simultaneous Group** (**SGSP**): the grouping is generated using the strategy of "**simultaneous events**" described above;
- **Data Analytics** (**DASP**): the grouping is generated using **data analytics** approaches as described above;
- **Operators Group** (**OSP**): the grouping is generated by the operator that groups 2 or more WS according to his/her experience.

Also SPs can have a Significance value associated to them that is computed using the Significance values of all the elements of the tree connected to it.

A possible approach to combine Significance values for an SP with 2 WSs contributing to it with significance S_1 and S_2 respectively, is derived from Certainty Factors (10) theory using the following formula

$$S(S_1\ and\ S_2) = S_1 + (1 - S_1) * S_2$$

Having more than 2 WSs contributing to the same SP, it is possible to iteratively apply the proposed formula as follows (in case of 3 WSs with Significance S_1, S_2 and S_3, respectively):

$$S_{1\ and\ 2} = S(S_1\ and\ S_2) = S_1 + (1 - S_1) * S_2$$
$$S_{1\ and\ 2\ and\ 3} = S(S_{1\ and\ 2}\ and\ S_3) = S_{1\ and\ 2} + (1 - S_{1\ and\ 2}) * S_3$$

As it is specified above, the idea is to build, whenever possible using the LEAs expert knowledge a tree of possible events (Weak Signals, Suspicious Events, Suspicious Patterns) happening at the venue on which reasoning on risk.

An example of a possible tree with WSs, SEs and SPs is given in Figure 1 while a detail of Suspicious Pattern SP6 with 4 WSs (each one with its own significance value) is provided in Figure 2.

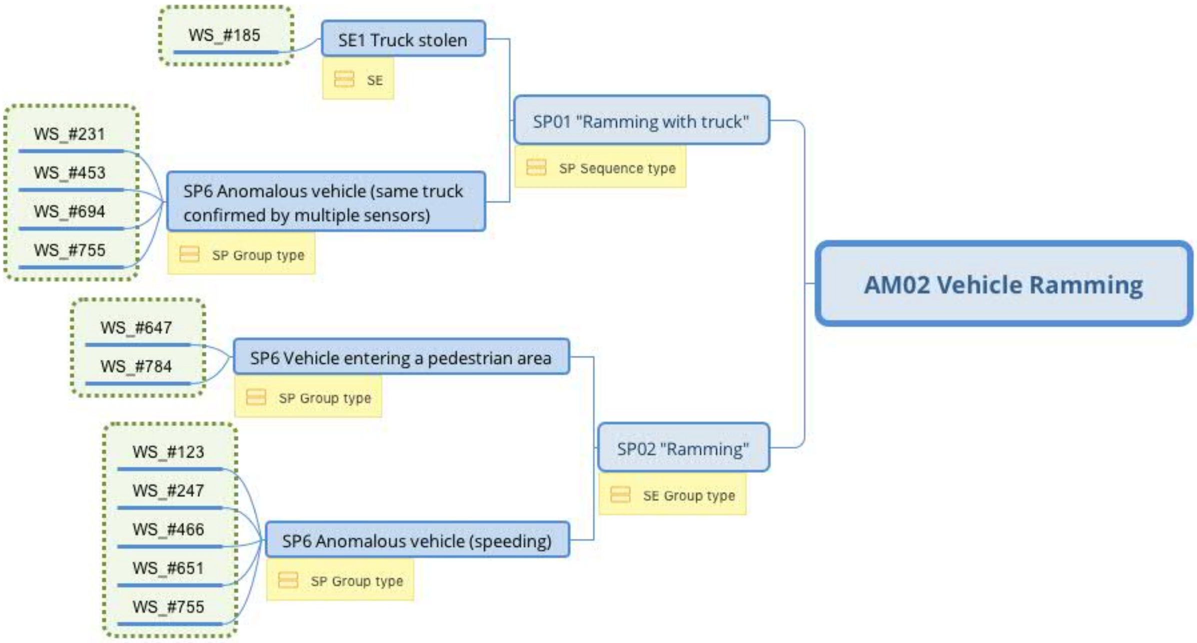

Figure 1 - Example of tree with SE, SP and AM

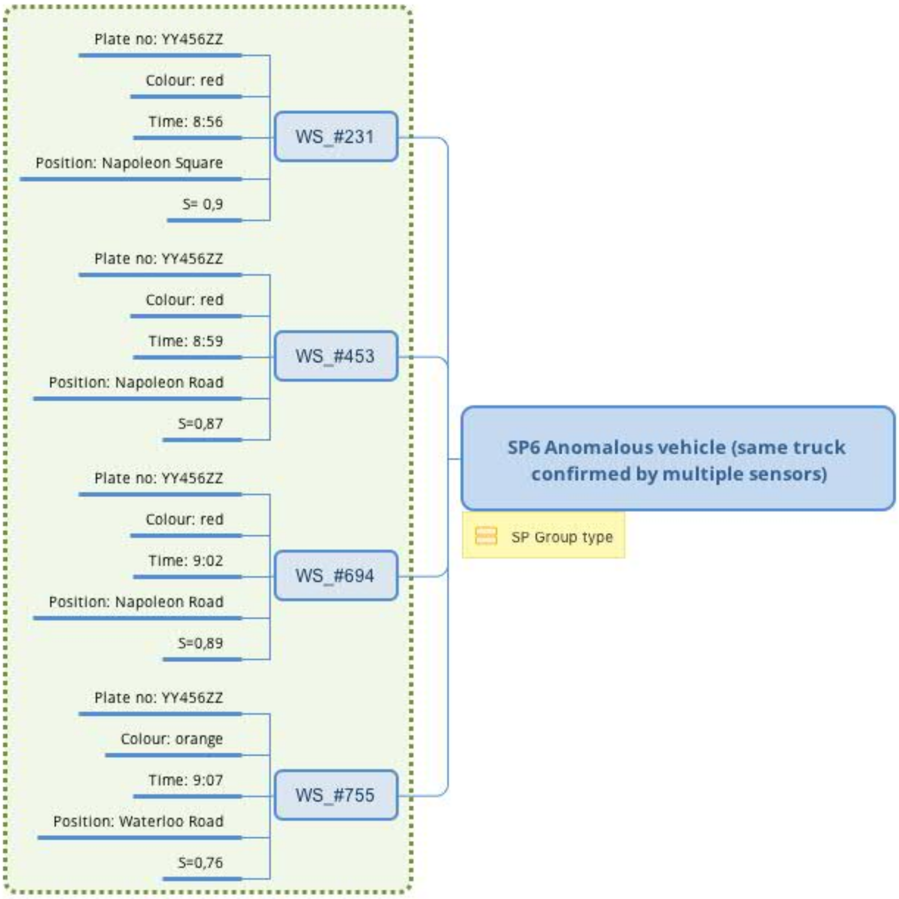

Figure 2 - Detail of the SP6 Suspicious Pattern

The Significance value of the Suspicious Pattern SP6 in Figure 2 is S_{SP6} = 0,9996568.

A more detailed example of the application of the DRA methodology with concrete numbers based on the Bilbao scenario is given in Section 6.1.3.

3.2.3 Critical elements

Suspicious Events and Patterns, when triggered by WSs, can be then classified as:

- **Non-Critical**, i.e. elements that do not constitute an immediate threat to the crowd;
- **Critical**, i.e. elements that constitute an immediate threat to the crowd.

Critical Suspicious Events and Patterns shall be brought immediately to the attention of the operator that should take the necessary mitigation actions.

3.2.4 Risk Level

Using the above methodology, the **Risk Level** can be computed using escalation approaches. A possible approach could be:

- IF (Time Distance from the event is Far) AND (no Critical SE or SP are triggered) THEN (the Risk Level is Very Low);
- IF (Time Distance from the event is Far) AND (some Non-Critical SE or SP are triggered) THEN (the Risk Level is Low);
- IF (Time Distance from the event is Far) AND (at least one Critical SE or SP is triggered) AND (Crowd Density is Low) THEN (the Risk Level is Medium);
- IF (Time Distance from the event is Close) AND (at least one Critical SE or SP is triggered) AND (Crowd Density is Low) THEN the Risk Level is High;
- IF (Time Distance from the event is Close) AND (at least one Critical SE or SP is triggered) AND (Crowd Density is High) THEN the Risk Level is Very High.

The proposed Risk Level could be referred to either the whole event or the specific attack modes.

Clearly, exact IF-THEN rules, thresholds and quantities need to be defined by LEAs according to their protocols, rules, experience including also socio-political and environmental conditions.

3.3 ADVANTAGES OF THE PROPOSED APPROACH VS. TRADITIONAL ANALYSIS

The advantages of situational awareness approaches like the LETSCROWD DRA are well summarised in the following Table 6.

Table 6 - Traditional analysis vs. LETSCROWD DRA

Traditional analysis	LETSCROWD DRA
Focuses on previous patterns	Searches for out-of-the-ordinary behaviour, allowing for detection of previously unseen threats
Time pressure drives toward premature closure	Allows memory of hypotheses and data rejected by security analysts
Analysts mostly operate on basis of own experience and biases	While introducing a semi-automatic approach, DRA leaves key analytic choices with analysts
Search tools mostly weed out what doesn't fit pattern	Notices what analysts are watching and asking

4 CREDIBILITY AND RELIABILITY OF SENSORS

4.1 INTRODUCTION

As reported in the Annex to STANAG 2022, Edition 8 (11) "*the aim of information evaluation is to indicate the degree of confidence that may be placed in any item of information which has been obtained for intelligence. (...) This is achieved by adopting an alphanumeric system of rating which combines a measurement of the reliability of the source of information with a measurement of the credibility of that information when examined in the light of existing knowledge*".

In STANAG 2022:

- the **reliability** characterises the source independently of the considered item of information;
- while the **credibility** introduces a measure of the degree of confirmation: the more an item of information is confirmed, the higher its credibility and, conversely, the more an item of information is contradicted by others, the less credible it becomes.

4.2 CREDIBILITY OF SENSORS

According to the definitions given in 4.1, credibility of the source clearly depends on the environmental conditions and the LEAs approach to collect the different sources of weak signals and therefore can only be evaluated after having analysed the outcome of the Practical Demonstrations (PDs).

4.3 RELIABILITY OF SENSORS

This section of the document evaluates the reliability of the sensors generating Weak Signals (WSs) considered in LETSCROWD:

- Human-Centred Computer Vision (HCCV);
- Web Crawler;
- Semantic Intelligence;
- Human as Sensor.

To express the reliability of the sensors the scale in Table 7 is applied.

Table 7 - The reliability scale

Value	Description
5	Very Reliable
4	Reliable
3	Quite reliable
2	Rather reliable
1	Less reliable

For the Human as Sensor the reliability scale is replaced by a more detailed discussion on the precursors considered and of the level of training (see Section 4.3.2).

4.3.1 WP5 tools

4.3.1.1 Human-Centred Computer Vision (HCCV) tools

Considering the HCCV tools delivered in WP5, Table 8 summarises the generated weak signals, the related precursors and the reliability of the tool to detect the precursors based on the feedback received by the developers to be assessed during PDs.

Table 8 - Reliability of HCCV-tools

Generated WS	Related precursors	Detection reliability
Estimated crowd density, from each of the available camera views	Crowd density does not represent, per se, a threat precursor. However, it can play an important role to determine consequences.	Reliability strongly depends on how much the images used to train the density estimator are representative of the operation scenario. In tests on benchmark, publicly available data sets where the density estimator was trained on the same camera views subsequently used for testing, the relative estimation error was around 10%, which can correspond to a reliability value of 4. This setting is however unlikely for LETSCROWD. In cross-database evaluations (training and testing images coming from different cameras and locations) the estimation error was sometimes much higher. To keep estimation error low (with a reliability value of 4) it is crucial to use a training set of images related to the ones acquired during operation: in the context of LETSCROWD this could be achieved by exploiting images or videos generated by the Crowd modelling tool of WP5.1, which is going to be tested in practical demonstrations.
Presence of a specific individual in different points of the event venue: first observed by a LEA operator on a given video, then automatically detected by the person re-identification tool in videos from the same or different cameras. Each detection has to be confirmed by a LEA operator to avoid false alarms	P01-P04 and P22-P26	The person re-identification tool works inherently with a man in the loop. If images of the individual of interest are present in the available videos and the software detects and returns them to the operator, then it can be assumed that the operator correctly recognises them. However, the pedestrian detection software may fail to detect a person, or the person re-identification software may place the images of the individual of interest far from the top of the returned list of images (possibly because they are not similar to the query image of the same individual, e.g., due to occlusions), which may prevent the operator from finding them (missed detections). These problems may happen in case of strong occlusions and low image quality (e.g., bad lighting conditions). Reliability should therefore be evaluated between 3 (for challenging operation scenarios) and 4: forthcoming practical demonstrations will suggest the most suitable value in the context of LETSCROWD operation scenarios.

Generated WS	Related precursors	Detection reliability
Detection of patterns of crowd movements and related anomalies - still under design	P09 and P19	This functionality is currently under design. The specific task of detecting anomalous crowd behaviours is known to be still very challenging for computer vision algorithms, and a man in the loop is required to check automatically generated alerts, to avoid false alarms. As in the case of person re-identification tools, missed detections can also occur. Therefore, a reliability value not higher than 3 is expected.
Detection of vehicles in the scene	P05 and P16	Current object detection software from images and videos are rather accurate in vehicle detection, including the one (based on deep learning) which is currently being used for pedestrian detection in the person re-identification and people search tools. A reliability value of 4 can be considered, to be confirmed after the forthcoming practical demonstrations.

All the weak signals produced by the HCV tool will carry geographical information, since they are associated to cameras whose exact position (as well as the location of the monitored scene) is assumed to be known.

4.3.1.2 Web Crawler

Generated WS	Related precursors	Detection reliability
Sensitive email addresses which may be found within the sources monitored by the crawler	P12	It depends on the source. An email found on INSTAGRAM may be less reliable (e.g. reliability = 3) than another found on PASTEBIN or somewhere else (reliability ≥ 4).
Leaked documents/emails which may be found within the sources monitored by the crawler	P12	5

In principle such weak signals are not carrying any geographical information.

4.3.1.3 Semantic intelligence

Generated WS	Related precursors	Detection reliability
The semantic engine includes an alarm mechanism that allows security analysts to configure the criteria that trigger an alarm. Each fired alarm is notified to the security analyst who in	P08	A tool like the semantic analysis engine can be fine-tuned for precision or recall, or a combination of both. A very precise system has a low recall, and a system with high recall has low precision. These systems are usually tuned for precision and recall at

Generated WS	Related precursors	Detection reliability
turn can send it as a weak signal to the PMT. An alarm tests, over a period of time, a list of conditions defined in terms of the semantic analysis output including: Number of web resources categorized in a taxonomy (e.g., crime taxonomy). Number of web resources mentioning a specific: Entity: Organization, Person, or places Term: word in general Number of web resources written with a minimum slang register: Crime, Cyber Illegal, or Military Therefore, the list of weak signals is dynamic and depends on the security analyst criteria.		the same time which leaves error margin along the two evaluation dimensions (precision and recall). Therefore, the output of the semantic analysis needs to be assessed by a security analyst. Rather than sending a weak signal for each fired alarm automatically the semantic analysis engine notifies a security analyst that is in charge of verifying the alarm content and decides whether to send a weak signal or not to the policy making toolkit. The security analyst must define the reliability of the detection based on the information provided by the system and his background knowledge.

4.3.2 Human as Sensor

While other sensors considered above, the Human as Sensor can potentially detect all possible threat precursors identified in Table 3, with different reliability.

To discuss the reliability of Human as Sensor, it is necessary, first of all, to define some typical categories of persons from which it is possible to receive WSs before or during a crowded event. The person's "reliability as a sensor" is based on the following basic skills:

- The level of his personal security awareness (citizens) – on average low reliability;
- The level of his security education in general (police officers) – on average medium reliability;
- The level of his specific education/training of suspicious signs in behaviour and appearance (police officers and stewards) – on average high reliability.

Training programs of suspicious signs are of different levels, starting from basic security awareness course (1-2 days) up to high level course of 4-6 weeks that includes all parameters that might indicate suspicious behaviour, cultural patterns, body language interpretations, simulations, on the job training and others.

The categories of "Specific Security Education" related to mass gathering events could be the following:

- Police officers and Stewards that have been subject to high-level training on detecting suspicious signs in behaviours and appearances;
- Police Officers with basic level of training on detecting suspicious signs in behaviours and appearances;
- Stewards with basic level of training on detecting suspicious signs in behaviours and appearances;
- Citizens without specific training on the matter, with some rare exceptions like Phoenix citizens (12).

For each category identified above, their "reliability as sensor" of suspicious signs is discussed in the following sections.

4.3.2.1 Highly-trained Police officers and Stewards

The ability of LEAs to identify suspicious signals and the consequent reliability of their reports varies according to the institutional tasks they are assigned to. In particular, on the basis of the tasks to be performed, each Police Officer receives specific training. The most trained operators with the best acquired professional experience (and therefore originators of the highest reliable reports) are those who have specific tasks such as those related to prevention and public rescue (in practice all crime street units and anti-riots squads).

Police officers and stewards which undergo targeted high-level training in identification of suspicious signs are considered the most reliable "human sensors" due to several reasons:

- They use techniques of identification of WSs learnt and simulated during their preparation course and on the job training;
- Usually the police officers and stewards employed in the mission are familiar with the local mentality, attitude and temperament of the citizens as well as the local environmental conditions and are efficient "sensors" in identifying bizarre circumstances that might indicate WSs;
- They are also familiar with rules, values, attitudes and behaviours of specific groups that usually attend mass gatherings (i.e. political subgroups, sportive supporters, fan clubs, etc.…);
- Police officers are employing techniques learned in other similar fields such as dealing with crimes and public disorder;
- Police officers gain experience from past events and therefore their reliability is increased through trial and error processes;
- Police officers are exposed to intelligence and threat information and know what to look for.

Sometimes, high-level trained stewards are very reliable sensors, being their role focused on limited tasks like searching the people, guiding the crowd, etc. while police officers are dealing with other tasks (public order, traffic and others). Moreover:

- They can be dedicated to the task of identifying suspicious signs during the event (while police officers are usually busy in many other tasks);
- Quite often they are ununiformed and therefore not recognized by the public as LEA;
- They can be of different gender, age etc., to be adapted to the type of the event;
- Even if usually they don’t have the official power to act, their reporting could be of very high importance.

4.3.2.2 Basic-trained Police Officers

All police officers receive basic training to detect suspicious signs, enriched by the day to day practice to detect people or things out of the ordinary. Moreover, officers work in their patrol area, with knowledge and proximity to the environment and people, which helps to detect possible suspicious signs. Every day, before leaving on patrol, in the briefing they receive information about what happened previously, crimes, perpetrators, victims, where, modus operandi, etc.

However, the basic specific training is considered as an enrichment/improvement of the basic police officers' skills and not as real education program like the high-level course. Therefore, Police Officers which undergo basic training on detecting suspicious signs in behaviours and appearances are considered as moderately reliable for the following reasons:

- They are lacking specific training in identification of suspicious activity even if their duties and police officers' training are in higher level than ordinary citizens.
- They are well suited to identify crime and public disorder activity rather than suspicious activity.

- They are not looking for the suspicious signs, nevertheless, once identified, they are able to deal with them.

4.3.2.3 Basic- and Medium-trained Stewards

As pointed out in Section 4.3.2.1, stewards, when properly trained, could be potentially extremely reliable in detecting suspicious behaviours.

However, the level of training for stewards managing crowded events is extremely heterogeneous across Europe and, in most cases, legislation and/or best practices do not foresee/prescribe the required level of training to detect suspicious behaviours or signs as shown by the following examples:

- The FIFA[2] Stadium Safety and Security Regulation (13), in the section devoted to stewards' training, refers to neither suspicious signs nor body language interpretation;
- The City & Guilds[3], a skills development company, offers a steward training course (Level 2) where the training units (14) are: prepare for spectator events, control the entry, exit and movement of people at spectator events, monitor spectators and deal with crowd problems, help to manage conflict, contribute to the work of the team, deal with accidents and emergencies;

  The only reference to the detection of suspicious behaviour is in a single module devoted to the identification of the obvious signs of the following types of crowd problems:

  - unexpected crowd movements;
  - local overcrowding;
  - over-capacity;
  - distress;
  - separation of individuals and groups;
  - unsociable behaviour;
  - unlawful behaviour;
  - entry into restricted areas;
- The Italian regulation[4] on the stewards for the football matches foresees a series of duties for the stewards (checking the tickets, avoiding the introduction of dangerous items using metal detectors, etc.) but nothing related to suspicious behaviours.
- On the contrary, a first interesting positive example is the training received by the stewards in charge of the FIFA World Cup thanks to the UEFA assistance to the Russian Football Union (FSU) in areas such as counter-terrorism measures and training stewards (15).

This means that reliability of stewards can change sensibly and cannot be taken for granted.

For the above reasons, LETSCROWD has decided to develop a training package for crowd protection based on human factor (D3.7) that includes specific modules dedicated to Suspicious Signs in Appearance and Behaviour and Suspicious Objects

4.3.2.4 Citizens

Citizens are the less reliable category amongst the considered categories, for a series of reasons:

[2] Fédération Internationale de Football Association

[3] https://www.cityandguilds.com

[4] Law Decree of the Ministry of Interior dated 8 August 2007 and its modification dated 24 February 2010

- Quite often they do not report suspicious signs to authorities. As reported in (16), the motivations for not reporting are various and strongly depend on the environmental conditions:
  - Some people simply do not realize that what they have witnessed might be a precursor of future violence or live in towns where suspicious behaviour may actually be the norm.
  - Other citizens cannot afford to interact with authorities, either since they are involved in illegal activities, or they hate authorities or even they are considered as "snitch" if they speak with police.
  - Others refuse to report to authorities for fear or since they do not want to be involved in others' business or do not see any obligation to contribute in any way to public security.
  - Others don't want to bother police with what at first glance doesn't seem important. They think that police have more important things to do and realise the importance only when something has happened.

The exception is a very small category of citizens: those who have basic awareness for security and safety. Usually they will keep away from the "threat" and in most of the cases, report to the first responders. In this category fall the being part of the following initiatives:

- The training and awareness courses for public workers like the PREVENT strand of the UK counter-terrorism strategy[5] (CONTEST), for which effectiveness of results is not yet fully assessed.
- The Community Awareness Program® (CAP®) designed in accordance with and in support of the Department of Homeland Security "If You See Something, Say Something" campaign and the national Suspicious Activity Reporting (SAR) process and training[6].

The reliability of the information received from citizens is already coded by many LEAs. An example is the coding used by the Belgian police (similar to many others in EU):

- Reliability information:
  - Heard and confirmed;
  - Heard and not confirmed;
  - Observed by source (who has passed on information);
  - Certain;
- Reliability source:
  - Reliable;
  - Mostly reliable;
  - Unreliable;
  - Not judgeable.

4.3.2.5 Human as a sensor: reliability scale

From all the above, it is possible to synthesise the reliability of the Human as a Sensor according to the scale shown in Table 9.

[5] https://www.gov.uk/government/publications/counter-terrorism-strategy-contest-2018
[6] https://www.thecell.org/cap/

Table 9 - Reliability scale of the human as a sensor

Position	Level of reliability
High-level trained Police officers and Stewards	5
Basic-trained Police officers	3-4
Citizens	1
Stewards	It can vary from 1 to 4 depending from the level of training of the stewards concerned.

This synthesis is purely indicative and can be modified according to country-specific level of training of the different categories of persons and the rules, practices and specific condition of each LEA.

5 RULES TO BE APPLIED TO BUILD SUSPCIOUS EVENTS OR PATTERNS

The tables below represent a set of possible rules to be used to group (cluster) Weak Signals into Suspicious Pattern according to what has been described in Deliverable D3.4 (17) section 4.2.2 and summarised also in Section 3 of this document.

Whenever possible, the rules are based on the detection of the Attack Modes and Threat's Precursors described in Section 2.2 (in brackets within the rule as Pnn).

The proposed rules will be translated into coded rules to be interpreted by the SW tool supporting the Practical Demonstrations

Table 10 - "Abandoned object" rule

Name	Abandoned Object
Type	SSP
Rule	IF Individual with a bag AND AFTER Bag left unattended AND AFTER Individual leaves the scene for a given time THEN Abandoned object
Threat(s)	Bomb/IED (AM04)
Parameter(s)	A time parameter (e.g. 10 minutes) must be set for the individual leaving the scene to avoid many false alarms (e.g. the individual return into the scene after 30" after having thrown a piece of paper in the bin).
Note(s)	The time interval represented by AFTER needs to be defined for each scenario. The Abandoned Object may become a Suspicious Object according to various possible environmental conditions and specific circumstances In many cases it is necessary to select only individuals with certain characteristics (e.g. age in a specific range).

Table 11 - "Suspicious Object" rule

Name	Suspicious Object
Type	SSP
Rule	IF Abandoned Object AND Abandoned Object NOT TYPICAL THEN Suspicious Object
Threat(s)	Bomb/IED (AM04)
Parameter(s)	NOT TYPICAL is an object that is not typical for the given environment (e.g. left by an individual that after placing it, is running away or the bag has signs of oil stains and/or wires) or the way in which it has been abandoned.
Note(s)	See previous rule. The distinction between abandoned and suspicious object differ from country to country, so these two rules could be modified to take into account local specificities (e.g. the time to wait until an object becomes an abandoned object).

Table 12 - "Suspicious car accidents" rule

Name	**Suspicious car accidents**
Type	SGSP
Rule	IF Car accident AND NEARBY Car accident AND NEARBY Car accident THEN Suspicious car accidents
Threat(s)	Three (or more) simultaneous car accidents may represent a tentative to block access (or evacuation) roads to the event place or to divert police officers from the event.
Parameter(s)	The car accidents shall be simultaneous (the time interval to define a sequence of events as simultaneous needs to be specified according to LEA's practices.
Note(s)	The NEARBY concept must be defined for each event (e.g. in one of the roads bringing participants to the event). The time frame should be very close to the event start.

Table 13 - "Suspicious Diversion Attack (similar responses)" rule

Name	**Suspicious Diversion Attack (similar responses)**
Type	SGSP
Rule	IF Explosion OR Fire far from event venue AND Explosion OR Fire far from event venue AND Explosion OR Fire far from event venue THEN Suspicious Diversion Attack
Threat(s)	Tactic used to draw LEA/first responders' resources away from the intended primary target (6)
Parameter(s)	The Explosions shall be simultaneous. The concept of far from event venue shall be defined by the LEA according to its practice/experience
Note(s)	The Explosion can be replaced by (a combination of) other events with similar effects: e.g. putting fire on rubbish container on the road, multiple hoax devices, etc. The time frame should be close to the event start.

Table 14 - "Testing Security" rule

Name	**Testing Security**
Type	GSP
Rule	IF Individual Taking Picture of Venue (P01) AND Individual NEARBY Sensitive Parts of the Venue THEN Gathering Sensitive Information
Threat(s)	All possible attacks

Parameter(s)	NEARBY shall return all positions from which it is possible to take pictures of sensitive parts of the venue place (see notes).
Note(s)	Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), or security-related equipment (perimeter fencing, security cameras), etc. (6).

Table 15 - "Suspicious Vehicle 1" rule

Name	**Suspicious Vehicle 1**
Type	GSP
Rule	IF Car Stolen (P17) WITH PLATE <plate no.> AND Car Stolen WITH PLATE <plate no.> APPROACHING Venue THEN Suspicious Vehicle
Threat(s)	Ramming or VBIED bomb attack
Parameter(s)	The NEARBY concept must be defined for each event (e.g. in one of the roads bringing participants to the event).
Note(s)	To make this rule effective, local legislation must allow “preventive” vehicle plate recognition

Table 16 - "Suspicious Vehicle 2" rule

Name	**Suspicious Vehicle 2**
Type	GSP
Rule	IF Overloaded Car (P06) AND Overloaded Car APPROACHING Venue THEN Suspicious Vehicle
Threat(s)	Ramming or VBIED bomb attack.
Parameter(s)	
Note(s)	APPROACHING concept is any area defined by the operator in which no suspicious car should be present. Overloaded car can be detected by Human as Sensor.

Table 17 - "Testing Security" rule

Name	**Testing Security**
Type	SGSP
Rule	IF False Alarm (belonging to a set of pre-defined behaviours and close to hot spots) AND False Alarm (belonging to a set of pre-defined behaviours) AND False Alarm (belonging to a set of pre-defined behaviours)

	THEN Testing Security (P29)
Threat(s)	Generic terrorist attack.
Parameter(s)	The False alarms shall be simultaneous.
Note(s)	The set of pre-defined behaviours.

Table 18 - "Suspicious Behaviour" rule

Name	**Suspicious Behaviour**
Type	SGSP
Rule	IF An individual is wearing a heavy coat on a hot day with both hands are in the pockets of the coat AND (after some time) The individual is loitering in the vicinity of the event entrance THEN Suspicious Behaviour (P22)
Threat(s)	Suicide bomber (AM01) or Cold steel (e.g. stabbing) (AM06)
Parameter(s)	Time parameter must be set before the start of the event, showing nervousness and trying to avoid contact with LEA.
Note(s)	Similar rules can be similarly defined using the other suspicious behaviours identified amongst the threats' precursors identified in Table 3 (e.g. those from P23 to P27).

Table 19 - "Evacuation Risk" rule

Name	**Evacuation Risk**
Type	SGSP
Rule	IF Crowd Density ABOVE Threshold AND Evacuation Time GREATER THAN Threshold THEN Evacuation Risk
Threat(s)	Not linked to a specific threat, but a potential risk of injuries and/or fatalities for the crowd.
Parameter(s)	The thresholds for the crowd density and evacuation time depend on the type of event, geo-spatial characteristics of the considered area and, more in general, environmental conditions.
Note(s)	The Evacuation Time can be computed in real time of pre-calculated for pre-determined crowd concentration areas (e.g. the area in front of a stadium's entrance).

Table 20 - "Suspicious Driving Behaviour" rule

Name	**Suspicious Driving Behaviour**
Type	GSP

Rule	IF
	Sequence of abnormal driving behaviours
	THEN

	Suspicious Vehicle
Threat(s)	Ramming or VBIED bomb attack
Parameter(s)	Pedestrian zone or red area
Note(s)	Pedestrian zone or red area should be fixed ahead. Possible examples of abnormal behaviours are driving against the allowed direction, passing a junction with red light, etc.

Table 21 - "Suspicious Theft" rule

Name	**Suspicious Theft**
Type	SGSP

Rule	IF
	Multiple thefts of chemicals in a short period of time, but far from event date
	THEN
	Suspicious Theft

Threat(s)	Ramming or VBIED bomb attack
Parameter(s)	Time defined by the operator between a set of days before the event.
Note(s)	The time frame should be very close to the event start.

Table 22 - "Suspicious Vehicle 3" rule

Name	**Suspicious Vehicle 3**
Type	GSP
Rule	IF Truck circulating AND Area/s not permissible to trucks (or in specific hours not permissible to trucks) THEN Suspicious Truck
Threat(s)	Ramming or VBIED bomb attack.
Parameter(s)	Area in city centre.
Note(s)	Not relevant for cars.

Table 23 - "Suspicious UAV Flight" rule

Name	**Suspicious UAV Flight**
Type	SSP or DHSSP
Rule	IF UAV (Unmanned Aerial Vehicles) CLOSE TO Hot Spots AND AFTER A Day UAV CLOSE TO Hot Spots THEN Dry Run
Threat(s)	Attack preparation
Parameter(s)	The detection of UAV can be done by the Human-as-Sensor
Note(s)	A recent proxy example is the escape from a French jail of the famous robber Redoine Faïd in July 2018 (18) that used drones to prepare its escape with a helicopter.

Table 24 - "Suspicious Cyber-Attack" rule

Name	**Suspicious Cyber-Attack**
Type	GSP
Rule	IF Cyber-Attack on Victim <A> AND Victim <A> of the Cyber-Attack BECOMES linked to the Event THEN Suspicious Cyber-Attack
Threat(s)	Attack preparation
Parameter(s)	
Note(s)	This rule highlights the possibility that a cyber-attack could compromise the resilience of the IT infrastructure of either the event organiser or the LEA in charge of protecting the event.

Table 25 - "Suspicious Data Breach" rule

Name	**Suspicious Data Breach**
Type	GSP
Rule	IF Data Breach on Victim <A> AND Victim <A> of the Data Breach BECOMES linked to the Event THEN Suspicious Data Breach
Threat(s)	Attack preparation
Parameter(s)	
Note(s)	This rule highlights the possibility that a cyber-attack (e.g. from an insider) could steal data owned by a company linked to the event (e.g. the company managing the stewards) thus putting at risk the security of the event.

Table 26 - "Diversion by Fake News" rule

Name	**Diversion by Fake News**
Type	GSP

Rule	IF
	Multiple explicit announcement of an imminent attack against a target
	THEN
	Possible Diversion by Fake New

Threat(s)	Attack preparation
Parameter(s)	The detection of multiple explicit announcements can be implemented with web crawler and semantic intelligence.
Note(s)	The recent strategy of the “gilet jaune” in France (19) of diverting police forces by fake announcement (they announce for days a new event in Versailles and police was prepared

	for that, while they suddenly change the location in Montmartre) could be used also by terrorists.

6 THE DRA SCENARIOS

The DRA scenario will be tested in Practical Demonstrations (PDs) by 3 LEAs:

- Ertzaintza (ERT) in Bilbao;
- Policía Municipal de Madrid as part of the Ajuntamento de Madrid (ADM) in Madrid;
- Hochschule für den Öffentlichen Dienst in Bayern (BayFHVR) in Fürstenfeldbruck (Munich).

Here below the scenarios that have been defined and refined in strict cooperation and agreement of the involved LEA.

6.1 DRA SCENARIO IN BILBAO (BY ERT)

6.1.1 Introduction

6.1.1.1 Linked event

The DRA scenario in Bilbao will be run in first quarter of 2019 and will be centred around one of two possible events that will happen in the town:

- The processions during the Easter Holy Week (18-22 April 2019)
- A football match at the San Mamés stadium during the same period.

The area in which the scenario will be run is defined in the following as Area of Interest.

6.1.1.2 PD approach

To allow a proper demonstration of the DRA without interfering with the normal LEA operations, the data related to the Bilbao scenario will be acquired during the real event and then simulated, after data cleansing, using the ETRA situational awareness SW.

The steps required to run the Bilbao PD can be summarised as follows:

1. ERT will
    a. Store approx. 1 month of events from its database (e.g. ZUTABE) representing the Weak Signals (WSs) to be processed;
    b. If possible (according to ERT rules), record video streams for the HCCV tools and distribute them to technical partners;
    c. Clean the stored WSs from all the security-/privacy-sensitive information (name of persons, agents, etc.);
    d. Send the cleaned WSs database to ETRA for its integration into the LETS-CROWD tool;
2. Once integrated into the LETS-CROWD tool, the WSs database will form the basis of the DRA demonstration by
    a. Inserting the specific fictitious WSs that are necessary to implement the selected scenario;
    b. Running the DRA logic to show the potential benefits;
3. The fictitious WSs can be generated by
    a. The HCCV tools after having processed the video streams collected during the event. These can be either fully integrated into the ETRA tool (preferred option) using a recorded video stream or manually inserted into the tool;

b. The "human as a sensor" using the ETRA mobile application with the time set at the "correct" sequence in the scenario;

c. The combination of web crawler and semantic intelligence using a semi-automatic approach;

d. Other sensors LEAs may be interested to use. Also in this case the level of integration with the ETRA tool has to be clarified;

4. The event selected by ERT will be monitored by the web crawler and semantic intelligence since at least 1 month before the event itself.

6.1.2 Scenario description

4 weeks before the event

T01 - DRA receives WS01 based on a citizen's phone call registered in the ZUTABE emergencies' database: "A black van with French number plate has been parked a week ago on Road A" (Road A is a road nearby the Area of Interest and therefore receives a special attention by ERT).

T02 - ERT commander decides to ask the nearby bank, the video recording of the last week to detect if something strange happened in the area.

T03 - DRA receives WS02 from VA applied on the video recorded by the bank: "Two individuals are entering and leaving the van twice in the same day placing 2 bags in the van each time".

T04 - DRA receives WS03 based on a call from the same citizen, 2 days after: "The same black van remains parked".

T05 - Using the existing rules, SP01 "Suspicious car" is created by DRA grouping WS01, WS02 and WS03.

T06 - The ERT operator is alerted by the DRA tool and decides to send a policeman to check the car.

T07 - The policeman goes to Road A and verifies the suspicious vehicle and by checking the number plate discovers that it is a car used to store goods by some citizens living in the neighbourhood. The policeman therefore sends a message to the User to discard SP01 being a nuisance alarm.

2 weeks before the event

T08 - DRA receives an Intelligence Alert IA01: "Risk of potential terrorist attack" that raises the alert level from 1 to 3.

T09 - DRA receives WS04 from VA: "A red truck is entering an area close to the Red Zone of the event" (in this case it remains a pure weak signal without follow-up, but if the same truck appears again many times it could become a suspicious pattern according to protocols).

T10 - DRA receives an Intelligence Alert IA02: "Car rental in Madrid has noted a non-returned yellow van with 6 wheels and plate number [2018 LET]".

T11 - DRA receives WS05 from VA: "Plate number [2018 LET] has been detected by the radar control on motorway AP08 nearby Bilbao". The car was speeding but the delay between the detection and the processing has not allowed to stop the car.

T12 - Using existing rules, DRA creates a new Suspicious Pattern SP02 "Suspicious car" grouping IA02 and WS05.

1 week before the event

T13 - DRA receives an Intelligence Alert IA03: "Terrorists present in the Bilbao area".

T14 - ERT decides to

a. Define, around the Area of Interest, the most internal perimeter in which vehicles are not allowed from the day before the event (Red Zone) and the buffer zone (Orange zone) in which only certain categories of vehicles are allowed from the day before the event (e.g. residents' cars, couriers' vans, etc.);
b. Set-up specific hidden CCTV-cameras equipped with VA;
c. After being activated by the Intelligence Alert IA03 (and authorised by a judge), a vehicle with automated OCR for registration plate number recognition of the Bilbao's Municipal Police (BMP) is patrolling the area around the Area of Interest and collecting all plate numbers to detect suspicious behaviours.

T15 - DRA receives WS06 from VA: "A brown truck is entering an area close to the Red Zone of the event".

T16 - DRA receives WS07 from VA: "A red van is entering an area close to the Red Zone of the event".

T17 - DRA receives WS08 from the OCR on-board the BMP vehicle "Plate [2018 CRO] present in the Orange zone" (the systems is obviously receiving all the plate numbers of all cars in the area).

T18 - DRA receives WS09 from VA: "A blue car is entering an area close to the Red Zone of the event".

T19 - DRA receives WS10 from the OCR on-board the BMP vehicle "Plate [2018 CRO] present in the Orange zone".

T20 - DRA receives WS11 from a steward of the stadium "A non-authorised person tried to enter the stadium with false credentials".

T21 - DRA receives WS12 from the OCR on-board the BMP vehicle "Plate [2018 CRO] present in the Orange zone".

T22 - Using existing rules, DRA creates the SP03 "Suspicious vehicle with plate [2018 CRO]" (simultaneous group SGSP), grouping WS08, WS10 and WS012 (the same car passing 3 times the same place in a short period - it could be a vehicle exploring the area).

T23 - The operator alerts the commander that authorises patrols to stop the vehicle with plate [2018 CRO] for a security check. The car is stopped, and the passengers are found with a camera with pictures of all the security installations of the Area of Interest.

T24 - DRA receives WS13 from a steward of the stadium "A non-authorised person carrying big back-pack tried to enter the stadium hiding himself in a group of organiser's workers".

T25 - DRA creates SP04 "Probing security" grouping (ASP) WS11 and WS13. The operator is alerted, the commander recognises the increased terrorist risk and escalates the level of alert from 3 to 4.

The day of the event, with crowd outside the stadium queuing to enter

T26 - DRA receives WS14 from VA counting people above a given threshold: "The crowd is becoming quite dense".

T27 - DRA receives WS15 from VA: "A yellow van with 6 wheels is violating the Red Zone of the event".

T28 - Using the existing rules, SP05 "Ramming vehicle" is created by DRA grouping SP2 and WS15.

T29 - The user is alerted by the DRA tool and decides, for example, to

a. Alert the policemen in the area close to where the yellow van has been detected;
b. Run the Real Time Evacuation (RTE) tool or a pre-computed simulation from the Crowd Modelling and Planning (CMP) tool to evaluate if the existing crowd (measured by WS14) can quickly evacuate the place and gets a negative answer;
c. Alert the policemen to stop the yellow van with any possible mean since the crowd cannot be evacuated.

d. Escalate the level of alert from 4 to 5.

6.1.3 The DRA calculation applied to ERT scenario: an example

To better explain the proposed DRA methodology, in the following is shown an example of its application using dummy (but realistic) values to Credibility and Reliability of sensors applied to the ERT scenario described in Section 6.1.2.

The example starts by defining, prior to start the scenario, the credibility of the different sensors involved: the proposed values are shown in Table 27.

Table 27 - Sensors' credibility for the DRA example

Sensors	Credibility
Citizen	2
HCCV behaviour	2
HCCV plates	5
HCCV vehicles	4
HCCV crowd density	4
Intelligence	5
Steward	5

In Table 28 the sequence of received Weak Signals or computed Suspicious Patterns and the related calculations is presented.

Table 28 - The DRA flow of data and related calculations

Time	Signal/Pattern	Sensor	Description	Reliability R	TD	Significance	Norm. Significance	Alert Level
T01	WS01	Citizen	Suspicious Vehicle	4	1	8	0,06	
T02								
T03	WS02	HCCV	Suspicious Behaviour	3	1	6	0,05	
T04	WS03	Citizen	Suspicious Vehicle	4	1	8	0,06	
T05	**SP01**	DRA Rule	Suspicious Vehicle	**WS01 & WS02 & WS03**			0,17	
T06	Patrol sent to check							
T07	SP01 deleted after operator's check							1
T08	IA01	Intelligence	Possible terrorist attack	5	2	50	0,40	3
T09	WS04	HCCV	Red truck	5	2	40	0,32	
T10	IA02	Intelligence	Stolen yellow van	5	2	50	0,40	
T11	WS05	HCCV	Suspicious plate detected	5	2	50	0,40	
T12	**SP02**	DRA Rule	Suspicious Vehicle	**IA02 & WS05**			0,64	
T13	IA03	Intelligence	Terrorist presence	5	3	75	0,60	
T14	Reaction due to IA03							
T15	WS06	HCCV	Brown truck	5	3	60	0,48	
T16	WS07	HCCV	Red van	5	3	60	0,48	
T17	WS08	HCCV	Suspicious plate detected	5	3	75	0,60	
T18	WS09	HCCV	Blue car	5	3	60	0,48	
T19	WS10	HCCV	Suspicious plate detected	5	3	75	0,60	
T20	WS11	Steward	Suspicious person	5	3	75	0,60	
T21	WS12	HCCV	Suspicious plate detected	5	3	75	0,60	
T22	**SP03**	DRA Rule	Suspicious Vehicle	**WS08 & WS10 & WS12**			0,94	
T23	Reaction due to SP03							
T24	WS13	Steward	Suspicious person	5	3	75	0,60	
T25	**SP04**	DRA Rule	Probing security	**WS11 & WS 13**			0,84	4
T26	WS14	HCCV	Quite dense crowd	4	5	80	0,64	
T27	WS15	HCCV	Yellow van	5	5	100	0,80	
T28	**SP05**	DRA Rule	Ramming vehicle	**SP02 & WS15**			0,93	5
T29	Reaction due to SP05							

At each step, according to the scenario described in Section 6.1.2, the following steps are implemented:

1) On the basis of the received WS, the corresponding values of sensor's credibility and reliability and the time distance from the event are identified.
2) The Significance is then computed using the formulas shown in Section 3.1 (with α, β and γ set to 1 for the sake of simplicity) and normalised to get values in the [0; 1] range.
3) Through the application of the DRA rules (see some examples in Section 5) the Suspicious Alert or Patterns are created and, if necessary, Alert Level is modified.

6.2 DRA SCENARIO IN MADRID (BY ADM)

The DRA scenario of the Ayuntamiento de Madrid (AdM) will be based on the LGBTIQ (lesbian, gay, bisexual, transgender, intersex and queer) Pride week on early July 2019.

Due to the complex decision-making process that took place to reach the final decision on the event to be selected (ended in mid-December 2018), more details on the specific DRA scenario will be reported in the D3.8 deliverable due at the end of April 2019.

6.3 DRA SCENARIO IN FÜRSTENFELDBRUCK (BY BAYFHVR)

6.3.1 Introduction

The DRA Practical Demonstration (PD) in Fürstenfeldbruck (Munich) will be implemented simulating a real event using the BayFHVR students as the crowd.

Simulated event: Visit of the ministry of interior at the school on T09 at 15:00.

Venue: BayFHVR premises in Munich. Estimated number of participants: 50-70.

6.3.2 Description of the scenario

The event is foreseen to be held in the assembly hall of the building. A group of extremists is planning to attack the event and to spread terror atmosphere due to the recent PAG[7] law.

Sequence of events:

T01 - The event is published on websites and in the local newspapers.

T02 - Hints from intelligence about potential extremism activity

T03 - A week after T01 LEA using crawler + semantic intelligence reports "dirty" debates in the social networks

T04 - A week after T03 – The Bavarian Intelligence Service[8] reports that the leaders of the NN movement have decided to activate the "Munich Cell" in order to attack the venue and create disorder, by placing and operating "smoke bombs" while the Ministry of Interior is speaking.

T05 - Few days after T04 – the CCTV system of BayFHVR reveals a student (Margarethe) taking pictures of the entrances to the parking lot, to the building and inside the hall. She was questioned by the security officer, explaining she wants to show the place where she studies to her parents, she will meet during the vacation.

[7] Polizeiaufgabengesetz – Police Responsibility Law

[8] Bayerisches Landesamt für Verfassungsschutz

T06 - Two weeks after T05 – at an apartment building in Hallstadtgasse 12 – a citizen reports to the fire brigades that he heard an explosion and saw smoke coming out the window of his neighbour's apartment. The apartment is empty, and the explosion happens inadvertently. Fire brigades entering the flat discover some extremist publication. The Bavarian Intelligence Service - is reinforced in its idea that something may happen, and the alert level is increased.

T07 - A week after T06 – Margarethe is applying for parking permission for an Opel Corsa with registration plate M-XY-123.

T08 - Few days after T07 Margarethe gets the parking permission

T09 - Few days after T08 just before the visit of the Ministry of Interior

a. 10:00 – the Opel Corsa enters the parking lot and parks occupying 2 spaces;

b. 10:15 - A policeman notices it after a while and checks the owner and discover that the car is stolen;

c. 10:30 – the Command & Control Centre of BayFHVR report to the police. The police are busy with many events the same day – and are delayed in their response;

d. 14:45 - Two men approach the parking lot, open the boot of the Opel Corsa, picking-up 2 identical bags;

e. 14:50 – they approach the entrance of the event with false press credentials and wearing hats;

f. The persons split up. Each of them goes to one side of the crowd;

g. The persons are constantly looking at their watches and nervously tapping on their bags;

h. At the exact same time the persons are placing the bags on the ground and leave the area;

i. A bag is discovered close to an exit door;

j. While the bag is checked, the evacuation simulation is run to evaluate the best direction of evacuation depending of the way through which the extremists have left, imagining the smoke bomb is a diversion for a more dangerous attack (e.g. shooting);

k. Individuals are back-tracked, found and arrested before they can attack.

7 CONCLUSIONS

This document represents one of the final steps of the development of the DRA methodologies offering all the necessary information for its implementation into a tool that will be implemented and demonstrated at the following LEAs sites:

- Ertzaintza (ERT) in Bilbao based on the Holy Weeks processions (18-22 April 2019);
- Ayuntamiento de Madrid (AdM), based on the LGBTIQ (lesbian, gay, bisexual, transgender, intersex and queer) Pride week on early July 2019;
- Hochschule für den öffentlichen Dienst in Bayern (BayFHVR), simulating a visit of the Ministry of the Interior at the school.

The document has added to the previous Deliverables D3.2 and D3.2:

- A revision of the DRA methodology to take into account the comments and suggestions received by the LEAs;
- An analysis of the sensors used to detect weak signals focuses on the evaluation of the reliability of each technology developed/improved in LETSCROWD (Human-Centred Computer Vision, semantic intelligence and web crawler) in detecting Weak Signals corresponding to specific threat precursors and on the reliability of different categories of human as a sensor in reporting suspicious behaviours: highly-trained police forces, basic-trained police forces, stewards and citizens;
- A series of rules, validated by the LEAs involved in the DRA, to increase the situational awareness of a LEA operator managing a crowded event. These rules are centred around the identification of possible simultaneous (in space and/or time) weak signals potentially interpretable as threat precursors (e.g. possible diversions like putting fire to garbage collectors on the road or simultaneous road accidents close to the event venue, simultaneous suspicious behaviours of some individuals, suspicious cyber-attacks to organisations that – after some time – become involved in the event organisation, etc.).

The proactive cooperation with the involved LEAs has allowed to reach a satisfactory level of development for the DRA methodology that has the following advantages over more traditional approaches:

- Searches for out-of-the-ordinary behaviour, allowing for detection of previously unseen threats;
- Allows memory of hypotheses and data rejected by security analysts;
- While introducing a semi-automatic approach, DRA leaves key analytic choices with analysts;
- Notices what analysts are watching and asking.

The details of the implementation together with some preliminary results obtained from the Practical Demonstrations will be reported in Deliverable D3.8 due at Month 24 (April 2019).

8 REFERENCES AND ACRONYMS

8.1 REFERENCES

1. **World Health Organisation (WHO).** *Communicable disease alert and response for mass gatherings: key considerations.* 2008.

2. **Cambridge University Press.** *Cambridge Dictionary.* [Online] https://dictionary.cambridge.org/dictionary/english/security.

3. **Endsley, M.R.** Towards a theory of situation awareness in dynamic systems. *Human Factors.* 1995, Vol. 37, 1, pp. 32-64.

4. **Schoemaker, P. J. H. and Day, G. S.** How to Make Sense of Weak Signals. *MIT Sloan Management Review.* 2009, Vol. 50, 3.

5. **Association of Chief Police Officers of England and Wales and Northern Ireland (ACPO).** *Counter Terrorism Protective Security Advice for Major Events.* s.l. : The National Counter Terrorism Security Office (NaCTSO), 2009.

6. **Office of the Director of National Intelligence.** Counterterrorism Guide for public safety personnel. [Online] 2018. https://www.dni.gov/nctc/jcat/index.html.

7. *Deep Abnormality Detection in Video Data.* **Vu, H.** Melbourne : Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17), 2017.

8. *Learning deep representations of appearance and motion for anomalous event detection.* **Xu, D, et al.** s.l. : BMVC, 2015.

9. *Learning temporal regularity in video sequences.* **Hasan, M., et al.** Las Vegas : 29th IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016.

10. **Lucas, P. J. F.** Certainty-factor-like structures in Bayesian belief networs. *Knowledge-Based Systems.* 2001, Vol. 14.

11. **North Atlantic Treaty Organization (NATO) Information Handling Services.** *Annex to STANAG 2022 (Edition 8).* 1992. DODSID, Issue DW9705.

12. **City of Phoenix.** Phoenix Neighborhood Patrol Program. *City of Phoenix.* [Online] https://www.phoenix.gov/police/neighborhood-resources/neighborhood-patrol.

13. **FIFA Fédération Internationale de Football Association.** *FIFA Stadium Safety and Security Regulations.* 2013.

14. **City & Guilds.** *Level 2 NVQ Certificate in Spectator Safety (QCF) (6852-02).* 2010. 500/8568/2, v.1.0.

15. **UEFA - Union of European Football Associations.** Key stadium security assistance to Russia. *UEFA.com.* [Online] 10 April 2018. https://www.uefa.com/insideuefa/protecting-the-game/security/news/newsid=2549061.html.

16. **Mc Bride, J.T.** Why People Don't Report Suspicious Behavior. *Law and Order.* [Online] Hendon Media Group, April 2016. http://www.hendonpub.com/resources/article_archive/results/details?id=5743.

17. **LETSCROWD Project.** *D3.4 LETS-CROWD ESM implementation guidelines for crowd protection Version 1.* 2018.

18. **Willsher, Kim.** French gang may have used drones before helicopter prison break. *The Guardian.* [Online] 2 July 2018. https://www.theguardian.com/world/2018/jul/02/french-gang-may-have-used-drones-before-helicopter-prison-break.

19. **Marin, L.** Acte 6 des Gilets jaunes: la manifestation se déroule à Montmartre plutôt qu'à

Versailles. *France Soir.* [Online] 22 December 2018. http://www.francesoir.fr/politique-france/acte-6-des-gilets-jaunes-la-manifestation-se-deroule-montmartre-plutot-qua.

20. **UK College of Policing.** Intelligence management - Research and analysis. [Online] 4 December 2014. https://www.app.college.police.uk/app-content/intelligence-management/analysis/.

21. **UK National Counter Terrorism Security Office.** Guidance - Recognising the terrorist threat. *GOV.UK.* [Online] 24 March 2017. https://www.gov.uk/government/publications/recognising-the-terrorist-threat/recognising-the-terrorist-threat#suspicious-items---guidance-for-staff.

22. **OASIS Consortium.** *Common Alerting Protocol Version 1.2.* 2010.

23. **Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS).** *Information Sharing Environment Suspicious Activity Reporting (ISE-SAR) Functional Standard.* 2015. V. 1.5.5..

24. *A Method for Selecting Optimal Number of Sensors to Improve the Credibility.* **Chen, Y., et al.** 8914769, s.l. : Journal of Sensors, 2016, Vol. 2016.

8.2 ACRONYMS

Acronym	Definition
ASP	Area Suspicious Pattern
C	Credibility
CBRN	Chemical, Biological, Radiological and Nuclear
CCTV	Closed-Circuit Television
CTI	Cyber Threats Intelligence
DASP	Data Analytics Suspicious Pattern
DHSSP	Distance from Hot Spots Suspicious Pattern
DL	Data Logger
DRA	Dynamic Risk Assessment
GIS	Geographic Information System
GSP	Group Suspicious Pattern
HCCV	Human-Centred Computer Vision
HS	Human as Sensor
IA	Intelligence Alert
IED	Improvised Explosive Device
JR	Juridical Recorder
KB	Knowledge Base
LEA	Law Enforcement Agency
OSP	Operator Suspicious Pattern
PD	Practical Demonstration
PS	Physical Sensor
R	Reliability
S	Significance
SE	Suspicious Event
SI	Semantic Intelligence
SGSP	Simultaneous Group Suspicious Pattern
SP	Suspicious Pattern
SSP	Sequence Suspicious Pattern
SRA	Static Risk Assessment
TD	Time Distance
UAV	Unmanned Aerial Vehicle
UK	United Kingdom
VBIED	Vehicle-Born Improvised Explosive Device
WS	Weak Signals