This report was funded by the European Union's Internal Security Fund — Police under grant agreement n° 815356

Public Resillience using Technology to Counter Terrorism

D3.1 Description of Best practices and Technologies

WP number and title	WP 3- **Technology assessment & Open Calls**
Lead Beneficiary	JADS
Contributor(s)	IGPR, TNO, DITSS, L3CE
Deliverable type	Report
Planned delivery date	30/11/2019
Last Update	12/12/2019
Dissemination level	PU

Disclaimer

The content of this report represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

The PROTECT Consortium consists of the following partners:

Participant No	Participant organisation name	Short Name	Type	Country
1	Dutch Institute for Technology, Safety & Security	DITSS	NPO	NL
2	KENTRO MELETON ASFALEIAS	KEMEA	RTO	GR
3	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO	TNO	RTO	NL
4	INSPECTORATUL GENERAL AL POLITIEI ROMANE	IGPR	GOV	RO
5	FORUM EUROPEEN POUR LA SECURITE URBAINE	EFUS	NPO	F
6	LIETUVOS KIBERNETINIU NUSIKALTIMU KOMPETENCIJU IR TYRIMU CENTRAS	L3CE	RTO	LT
7	GEMEENTE EINDHOVEN	Eindhoven	GOV	NL
8	AYUNTAMIENTO DE MALAGA	Malaga	GOV	SP
9	DIMOS LARISEON	DL	GOV	GR
10	VILNIAUS MIESTO SAVIVALDYBES ADMINISTRACIJA	VMSA	GOV	LT
11	MUNICIPIUL BRASOV	MUNBV	GOV	RO
12	STICHTING KATHOLIEKE UNIVERSITEIT BRABANT	JADS	RTO	NL
13	MINISTERIO DEL INTERIOR	MIR	GOV	SP

To the knowledge of the authors, no classified information is included in this deliverable

Document History

VERSION	DATE	STATUS	AUTHORS, REVIEWER	DESCRIPTION
V0.1	17/10/2019	First draft	JADS	ToC
V0.2	15/11/2019	Draft	TNO	Technologies description
V0.2	15/11/2019	Draft	IGPR	survey towards related EU projects
V0.3	20/11/2019	Draft	JADS	Combining phase
V.0.4	22/11/2019	Draft	JADS	Combining phase
V.0.5	29/11/2019	Draft	JADS	Primary final version
V0.6	06/122019	Draft	JADS	Submitted for review
V0.7	10/12/2019	Draft	George Kioumourtzis (DITSS)	Final review and Quality assurance
V1.0	12/12/2019	Final Draft	Patrick Padding (DITSS)	Final approval and submission

Definitions, Acronyms and Abbreviations

ACRONYMS / ABBREVIATIONS	DESCRIPTION
MB	Managing Body
PRoTECT	Public Resilience using Technology to Counter Terrorism
VAT	Vulnerability Assessment Tool
LDA	Latent Dirichlet Allocation
SLR	Systematic Literature Review
ENLETS	European Network of Law Enforcement Technology Services
GTD	Global Terrorism Database
PSOI	Public Space of Interest
UAV	Unmanned Aerial Vehicle-Drone
WP	Work package
LEA	Law Enforcement Agency
EMS	Emergency Management Services
FRs	First responders
IPR	Intellectual property rights
AI	Artificial intelligence

Table of Contents

List of Figures

List of Tables

Executive Summary

Deliverable 3.1 constitutes the first tangible outcome of WP3 whose aim it is to capture and assess the technology landscape underpinning the PRoTECT project.

In this deliverable entitled “Description of Best practices and Technologies” we will distill industry-strength tools as well as good/best practices based on a systematic literature review (SLR) with a focus on protection of public spaces in safe and secure cities;

In particular, this deliverable reports on the results of a systematic literature review on the state-of-the-art and the state-of-practice of technologies, methods and techniques, and associated good- and best-practices for the protection of urban spaces. In addition, it collects previous efforts in the protection of public spaces and previous work from the ENLETS network and EFUS members. Research results from previous H2020 projects and with high TRL level (6 and above) have been assessed as part of our technology evaluation framework that will be developed in the remaining deliverables of WP3.

The deliverable is organized in four logical parts in order to analyze, contrast and evaluate the urban space security techs and solutions from three points of view.

In part I, this deliverable reports on the systematic literature review provides the state of art regarding technologies, techniques and design solution for the protection of urban areas. We have taken into consideration not only academic outlets, but also, “grey” literature stemming from industrial papers, reports, outlets, websites, etc. Part II collects and analyzes the best practices from the LEAs in EFUS cities based on a survey. The literature survey is then complemented in part III with a thorough overview of the projects from the European-Community to further analyses and understand show the problem of protecting public spaces we face, as well as initial results from the identified projects. Lastly, there is an overview of existing commercially available technologies for different threats to protect urban spaces.

1 Introduction

After the attack on the Twin Towers in 2001, the world faced the sad existence of terrors and terrorists. Statistics from GTD in **Invalid source specified.** say that from 2012 till 2019, after an escalation of terroristic attacks, in 2018, we have seen the fourth consecutive year of declining global terrorism since terrorist violence peaked in 2014. Iraq suffered more terroristic attacks than all the other countries, and finally, in 2018, the people killed by terrorists decreased to 78%. On the other side in 2015, 2016, and 2017, multiple terroristic events influenced Western Europe's life. We still clearly remind the attacks carried out by jihadists in Paris, Brussels, Nice, Berlin, Manchester, London, and Barcelona. In 2018, probably the most cowardly attack ever seen the Islamic State assault the Christmas market in Strasbourg, France, killing five people and injuring 11 others. The deadliest series of attacks in 2018 occurred in Bandundu, Democratic Republic of Congo in December. Members of the Batende tribe attacked the Banunu community in four towns in Yumbi territory. Below in Figure 1, the statistics from the latest report from GTD.

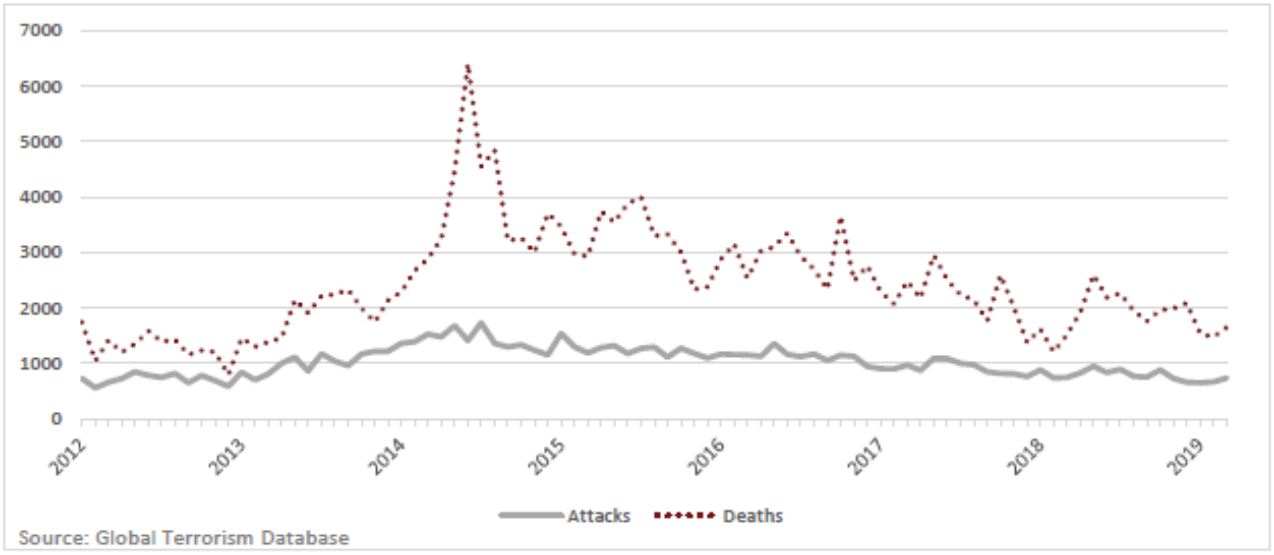


Figure 1 Terrorist Attacks and Total Deaths Worldwide, By Month, 2012 – 2019 (Q1)

Due to the violence and the terror atmosphere described by statistics from above, all the nations, municipalities, and LEAs started their running to solutions and technologies in order to mitigate, prevent, and avoid the attacks. I.e., for the Christmas market in Strasbourg this year they highly increased security and protection measures, 400 security cameras, all trams and bus stations in the city center are not served during market opening hours, no access to the parking places and car parks in the city center, 16 access bridges, identity check everywhere in the city center, obstacles have been installed to reduce the risk of car-rams[1]. The Christmas market in Strasbourg is only one example of the measures adopted by a municipality in order to increase the security level of citizens. As the example of Strasbourg, also all the other municipalities in Europe are nowadays looking at new technologies, methods and architectural solutions to increase the level of security in the cities. The deliverable 3.1 tries to give a broader overview of what are the new methodologies, solutions, and technologies for the protection of public spaces. Deliverable 3.1 claims to build a little encyclopedia that at 360 degrees can let municipalities, LEAs, and governments choose the

[1] https://int.strasbourg.eu/-/strasbourg-christmas-mark-1, http://www.rfi.fr/en/france/20191122-france-christmas-market-strasbourg-terrorism-tourism

appropriate solution based on the type of risks. The main intent of the deliverable is to focus on all types of treats that can happen in a city and find the appropriate solution to avoid them.

1.1 Introduce the P-Cube

This model has been adopted as the generally accepted framework for internal control and is widely recognized as the definitive standard against which organizations measure the effectiveness of their systems of internal control.

The identification, collection, assessment and benchmarking of technologies, best practices and needs for improved public space security is grounded on a framework, named the P-Cube, which has been inspired by the COSO model that is a widely accepted general-purpose control-driven framework for the auditing and compliance of technologies.

The P-Cube encompasses three orthogonal, yet correlated, dimensions:

1. Scenarios. The first dimension captures real-world scenarios with actual experiences about the usage of technologies of any kind to predict, avoid and/or reduce the likelihood of a vulnerability in a public space in a city or rural area to occur.
2. Technologies. This dimension encompasses techniques, tools, and methods (“cookbooks”) that are deployed in or around public spaces for the purpose of detecting threats/vulnerabilities, monitoring them, and analyzing and evaluating them in terms of the data-traces they leave behind (including video and audio footage, picture, tweets, narratives, etc.) for the purpose of mitigating the risk of security threats including terrorist threats and other malicious acts;
3. Vulnerabilities. The third dimension plots the urban context in which criminal and/or terrorist activities occur is itself characterized by points of vulnerability that can be attacked. The open and volatile nature of cities, the existence of key critical infrastructures and the closeness of big numbers of people in crowded spaces, all combine to present a set of attractive targets that are structured along the axis of this dimension in terms of discrete vulnerabilities that may occur. Examples include, but are not restricted to, fire arms attack, sharp object attack and vehicle attack.

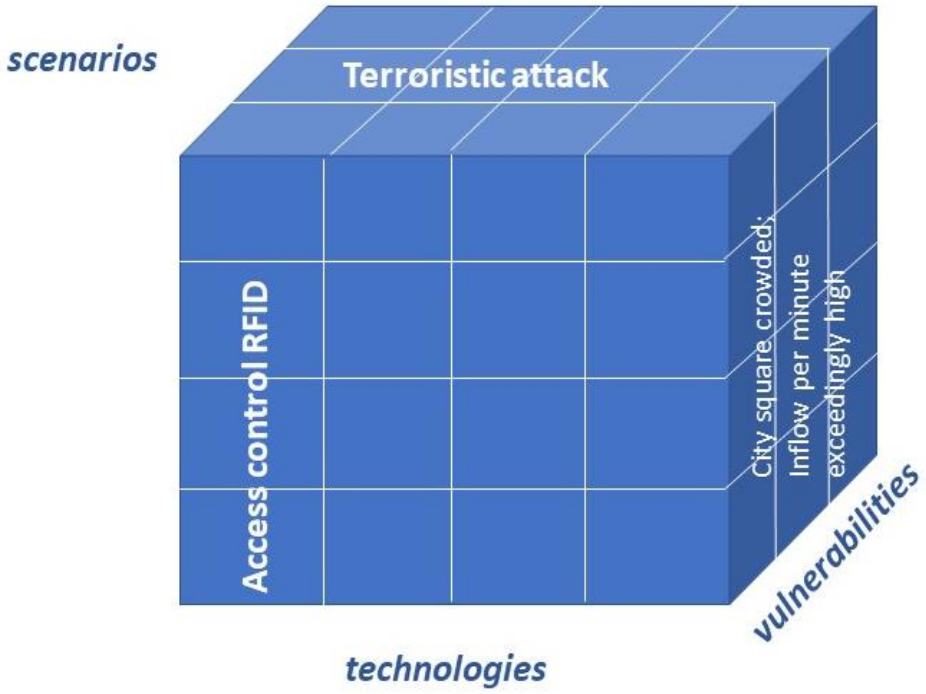


Figure 2 P-Cube in Action

Figure 2 graphically depicts the P-Cude in action using a simplified, yet realistic, real-world scenario that involves the protection of a city square during a mid-summer, pop-event involving 2,5k attendants.

Example:

Scenario (based on best practice in City – X): Terroristic attack in a city square during a pop concert.

Vulnerabilities:

- City square grounds are overly crowded;
- Weather conditions can change quickly (risk of severe thunder storms);
- Inflow per minute is exceedingly high.

Technology: Access control RFID wrist bands and Camera's to count people accessing.

1.2 Structure of this deliverable

This deliverable is structured as follows. In Paragraph *Literature study on relevant Technologies and Best practices* are fleshed out the solutions proposed by the scientific community for the protection of urban spaces. White and grey literature have been scraped in order to find all the scientific studies, industrial papers, reports, outlets, websites proposing new techniques to address the problem of protection of public spaces.

In Paragraph *Best practices from Cities and LEAs,* we look at what are the current and proposed solutions used by LEAs in order to guarantee safety and security in public spaces. We build a questionnaire that has been disseminated among all the ENLETS experts.

We then depicted state of the art of European Community finding all those projects related to the protection of urban spaces.

Lastly, in Paragraph *Overview of technologies,* we provide an overview of current technologies available on markets.

2 Literature study on relevant Technologies and Best practices

This chapter presents the results of a multi-vocal, structured analysis of scientific and industrial papers on technologies to mitigate vulnerabilities in the protection of public places. In addition, it lists and analyses best practices on safety and security of (semi-) public places in conjunction with applied technologies.

2.1 Introduction

2.1.1 Vision and Scope

Nowadays, terrorist attacks represent one of the major concerns for any nation (Clutterbuck, 1990). Indeed, in some areas of the world, civil servants and municipalities have to confront such threats almost on a daily basis. For example, focusing on the EU, in 2015 alone terrorism hit the headlines six times, specifically, the attacks in Paris, including the headquarters of Carlie Hebdo and the Bataclan Theater, resulting in 138 people killed and 413 injured (Boutry, 2019) (Rodionova, 2016) ---analysts deemed the criticalities of those attacks as connected to intelligence failure (Rodionova, 2016)---but the following years did not exhibit a better fate (Brussels explosions: What we know about airport and metro attacks, 2016), (Christmas attack: German government admits mistakes in aftermath, 2017), (Manchester Arena bomb: Service marks second anniversary, 2019), (Hache, 2016), (Kommenda, et al., 2017). Europol reports that in a time span of 4 years, 766 terrorist attacks occurred in with 205 attacks in 2017 respectively (EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT 2018 (TESAT 2018), 2018). In the same period 4072 suspects were arrested before or after the attack. Figure 3 below shows the number of attacks from 2014 to 2017 (EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT 2018 (TESAT 2018), 2018).

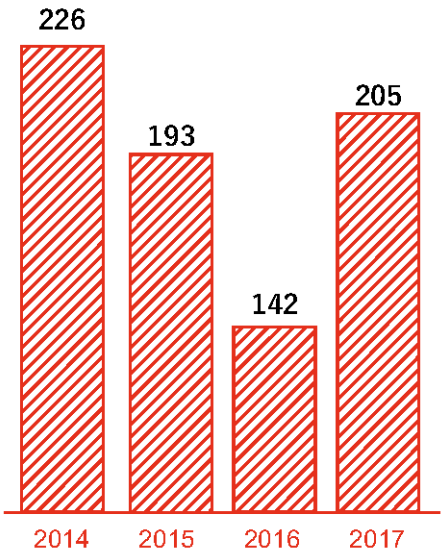


Figure 3 Number of failed, foiled or completed attacks from 2014 to 2017.

At the same time, from an economic perspective, the RAND Europe study, commissioned by the European Parliament to the RAND research organization, calculated in 2018 that the 28 EU member states lost around 180 billion in GDP terms due to terrorism between 2004 and 2016 alone, while the cost are potentially even higher, as data for an all-inclusive and comprehensive analysis is lacking (The cost of terrorism in Europe).

The single common denominator in all of the above facts is technology. Technology plays a paramount role in the prevention, protection, and preparation against terrorist attacks. Although back in 2004, Popp et al. summarize the different information technologies and domains for counter-terrorism \cite{popp2004countering} since then, technologies evolved and new technologies emerged, making the existing overview outdated and of limited practical usage.

This paper aims to provide an updated and timely overview of the state of the art in counter-terrorism information technologies; our investigation accounts for both grey and white literature on the matter with a systematic multi-vocal literature review (Garousi, Felderer, & Mäntylä, 2016), (Kitchenham, et al., 2009). Our analysis builds further on the observations and outline of information technologies already identified by Popp et al. in 2004 (Popp, Armour, Numrych, & others, 2004).

The main contributions of this paper are many fold; (a) providing an overview of state of the art in the current information technologies based on a systematic literature review (SLR); (b) quantitative indicators for further risk assessment and research in underdeveloped technologies; (c) a clear overview of the different techniques, prevention measures, methods of assessment for targeted information technologies; (d) best practices adopted by governments and private organizations.

2.2 Background and Related Work

The systematic literature review presented in this work is partially built on the paper by Popp et al. (Popp, Armour, Numrych, & others, 2004). However, due to technological advancements, a more elaborated taxonomy about the different best practices and information technologies related to the protection of urban space can be provided in this paper.

Popp et al. in (Popp, Armour, Numrych, & others, 2004) define 15 different information technologies that apply to the protection of urban space. To verify the existence of the technologies in literature and to exploit possible newly emerged technologies, our systematic literature review analyze the state of the art of the current best practices and information technologies for the protection of urban space. We took into consideration sources from the web such as blogs, news articles and product publications due to the novelty of specific technologies and the fact that a lot of these technologies also emerge in the private or corporate domain.

2.2.1 Terms and Definitions

In Table 1, all terms and related definitions used in this study are mentioned. The table consists of two columns: *Terms*, where the terms which are less commonly known and more technical are mentioned. In the second column *Definitions*, a short explanation is given to help better understand the essence of the mentioned term.

Terms	Definition
Biometrics	Identify and or verify human terrorist (or watchlist) subjects using 2D and 3D modeling approaches over a variety of biometric signatures: face, gait, iris, fingerprint, voice. Also exploit multiple sensor modalities: EO, IR, radar, hyper-spectral (Popp, Armour, Numrych, & others, 2004).
Clustering	Employ numerous technical approaches (natural language processing, AI, machine learning, pattern recognition, statistical analysis, probabilistic techniques) to automatically extract meaning and key concepts from (un)structured data and categorize via an information

	model (taxonomy, ontology). Cluster documents with similar contents (Popp, Armour, Numrych, & others, 2004).
Event detection	Monitor simple and complex events and notify users (or applications) in real time of their detection. Monitoring can be scheduled a priori, or placed on an ad hoc basis driven by user demands. When an event is detected, automatic notifications can range from simple actions (sending an alert, page, or email) to more complex ones (feeding information into an analytics system) (Popp, Armour, Numrych, & others, 2004).
Geospatial	Fuse, overlay, register, search, analyze, annotate, and visualize high-resolution satellite and aerial imagery, elevation data, GPS coordinates, maps, demographics, land masses, political boundaries to deliver a streaming 3D map of the entire globe (Popp, Armour, Numrych, & others, 2004).
Grey literature	Research that is either unpublished or has been published in non-commercial form. Examples of grey literature include: government reports. Policy statements and issues papers (New England, 2019).
Machine Learning	The science of making computers learn and act like humans by feeding data and information without begin explicitly programmed.
Semantic Consistency	Exploit ontologies, taxonomies, and definitions for words, phrases, and acronyms using a variety of schemes so users have a common and consistent understanding of the meaning of words in a specific context. Resolve semantic heterogeneity by capitalizing on Semantic Web technologies (Popp, Armour, Numrych, & others, 2004).
White literature	Research that has been published by an established scientific organization.

Table 1 Terms used and their definitions.

2.2.2 Related works

As previously mentioned, the first work to address the objectives behind this research is in Popp et al. (Popp, Armour, Numrych, & others, 2004); the authors provide an analysis on what was currently known about countering terrorism through information technologies. The goal of this paper is offer an updated, deeper analysis stemming from the same concepts and definitions (Popp, Armour, Numrych, & others, 2004). Popp et al. identify 15 information techniques most vital to preventing and countering terrorism attacks; the research focused on collaboration, analysis, and decision support tools, foreign language speech and text analysis tools, and pattern analysis tools to analyze and solve complicated terrorism related problems more efficiently and effectively. The study concluded that the three core IT areas, were not merely close to the whole of knowledge available on countering terrorism and many other information technologies are important for successfully countering terrorism (Popp, Armour, Numrych, & others, 2004). To help validate the usefulness and merits of these techniques, this study is aiming to map the available knowledge, going beyond the cataloguing of such knowledge but delving into a deeper layer of analysis on top of what was known.

In (Tounsi & Rais, 2018) Tounsi and Rais analysed the open source threat intelligence tools and the related performance. They then compare the features of the open source/free tools taken into account for the research against those of the tech company AlliCERT. From the research they found that some tools are focusing more on scalability and on celerity in facing zero-day exploits, using fast ways to exchange threat information, meanwhile, other tools are focusing more on the meaning of this information by applying big data analytics.

Besides analyses concerning online available information regarding information techniques, research has also been conducted on more in depth topics like the study of Zabłocki et al in (Zabłocki, Gościewska, Frejlichowski, & Hofman, Intelligent video surveillance systems for public spaces – a survey, 2014). In 2014, Zabłocki et al. conducted a survey on the latest state-of-the-art intelligent video surveillance systems and its most desirable features and characteristics. After analyzing and evaluating the video surveillance systems on several categories like on object detection and detecting and identifying abnormal and alarming situations, the study concluded that there are several challenges still to overcome. These challenges involve legal and privacy protection, difficulties with object movement analysis for occlusion handling and synchronization of multiple camera views during real-time system operation (Zabłocki, Gościewska, Frejlichowski, & Hofman, Intelligent video surveillance systems for public spaces – a survey, 2014).

Differently from the studies in (Tounsi & Rais, 2018) and in (Zabłocki, Gościewska, Frejlichowski, & Hofman, Intelligent video surveillance systems for public spaces--a survey, 2014) where the target of the analysis was a subset of the available methods and techniques to protect public spaces (open source/ free tools and video surveillance systems) we aim at mapping a wider range of studies regarding the prominent information systems and techniques used to protect urban areas and thereby helping to point out the strengths and weaknesses of current information techniques.

3 Research Materials and Methods

This Systematic Literature Review aims to provide an inclusive overview of the current state of the art in the information techniques that aid in the protection of urban spaces. We decided to conduct a systematic multivocal literature review to include grey literature in the overview of results, this is due to the fact that most of the research in this field have been conducted outside the scientific research domain.

The next section provides an overview of the methods used for obtaining the white and grey literature and provides the research questions and means that are employed to obtain the final results.

3.1 Research Questions and Approach Overview

The main research question behind this work:

"What are the best practices and technologies available nowadays for the protection of physical spaces?"

In order to address the above research question, we adopt the well-known Systematic Literature Review (SLR) research approach (Kitchenham, et al., 2009). More specifically, first we sample online literature in order to provide an overview of the techniques, technologies, and tools used for the protection of urban spaces. Subsequently, by means of unsupervised Machine-Learning analysis techniques specific for topic modelling and literary analysis (Onan, Korukoglu, & Bulut, 2016) (Williams & Betak, 2018) as well as content analysis (Krippendorff, 1980) (Hsieh & Shannon, 2005), we gather indicators for (1) further assessment over the technologies and information systems found in literature as well as (2) identification of any existing gaps in the scientific literature.

One of the key feats of our study is its harnessing of *grey* literature (Garousi, Felderer, & Mäntylä, 2016), intended as a more traditional literature and in general not submitted to peer-review and disseminated outside the scientific academic channels, including "*reports (annual, research, technical, project, etc.), working papers, government documents, non-government documents, white papers, and evaluations*".

The remainder of this section outlines all the above phases and the techniques adopted within them in more detail.

3.2 Sample Section and Control Factors

To limit the span of this research, selection criteria are applied to the white papers found. The inclusion criteria consist of:

Case	Criteria
Inclusion	i_1) The study discusses methods or technologies to address the topic.
	I_2) The study discusses the challenges around the topic close to our RQs.
	I_3) The study addresses know-how, guidelines or best practices on the topics in our RQ by directly-experienced LEAs, municipalities or practitioners.
	I_4) The study reports a case-study of urban space attack incidents or approaches.

Exclusion	E_1) The paper does not discuss sufficient details on implementation of practices, methods or tools for protection of urban spaces. E_2) The discussed topics are not explained or evaluated by the paper. E_3) The research paper does not discuss scope and limitations of the proposed frameworks, methods, tools, solutions, guidelines.

Table 2 Inclusion and exclusion criteria for sample selection.

The inclusion criteria (I_1 - I_4) represent the parameters we used in order to identify the targets of our study. On the other side the exclusion criteria are in charge of exclude papers that do not match our targets, i.e. E_1 to exclude studies with poor design/implementation details or E_4 in order to exclude studies that do not examine limitation and impact of the proposed solution.

The study needs to satisfy all the inclusion criteria in order to be added, while is excluded if it satisfy at least one exclusion criteria.

Based on the criteria stated in table Table 2 we selected 85 papers for the white articles and 27 grey articles. For the screening process we used not only the inclusion and exclusion criteria but also our quality control factors explained in the following.

- articles after 2004,
- the articles must be written in English,
- governmental websites have been scraped in order to find further research.

The research of Popp (Popp, Armour, Numrych, & others, 2004) provides the foundation of this research. In order to guarantee the most up-to-date information, articles after 2004 are included into this research. The next criterion, that all articles used must be written in or translated into English. This in order to ensure the quality of the content and allowing it to be replicable. Finally, since information about information technologies in the context of countering terrorism or the public's safety not only exist in papers, governmental websites are used within the scope of this research. Indeed, we truly believe that the governmental websites are good sources since they are expected to be unbiased and consist of checked facts.

The grey papers were selected online with less strict criteria than the white papers and mainly following those in Table 2. This is because grey articles are defined as "*research that is either unpublished or has been published in non-commercial form. Examples of grey literature include: government reports. policy statements and issues papers"* (New England, 2019).

3.3 Search strategy

We narrowed results obtained from our search string to industrial, government, and non-governmental paper researches (e.g., blog articles, white papers, magazines) published from 2004 until 2019. Google (primary) and Bing are the two search engines we decided to use.

At the same time, to cover for white literature appropriately, we run our queries in typical and most common computing literature libraries, namely: (1) ACM Digital Library; (2) IEEEXplore; (3) Wiley Interscience; (3) Elsevier Scopus; (4) Bibsonomy (5) Google Scholar; and (6) and Science Direct. Adjoining the stated online library databases, references from articles found and/or the corresponding journals may be used to gather information.

In order to address the *Inclusion* and *Exclusion* criteria above mentioned we defined the necessary keywords to be used to find our white and grey literature. A keyword search is a search type that checks for matching documents involving one or more words specified by the user. These keywords need to discriminate the most relevant research among the scientific databases (Sarı, Tosun, & Alptekin, 2019). Keywords, displayed in Table 3, are those used for searching in the databases listed above. We combined multiple keywords in order to enhance the search results by filtering out irrelevant articles. In Table 3 the list of the keyword used for this literature review.

Keywords:		
Biometrics	Filtering	Publishing
Categorization	Geospatial	Resolving terms
City	Government	Safety
Clustering	Information management	Searching
Context management	Information technology	Secure
Counter terrorism	Infrastructure	Semantic consistency
Crime	Knowledge management	Terrorism
Data	Machine learning	Urban
Database processing	Predictive modelling	Video processing
Event detection	Prevention	Visualization
Event notification	Public space	Workflow management

Table 3 Table of keywords used.

3.4 Data extraction

For the extraction of the data, a mixed-method analysis approach was used to obtain qualitative and quantitative data at once (Johnson & Onwuegbuzie, 2004). For this, a thematic coding method was applied to generate themes from the involved data. The thematic coding was done in a six-phase analysis method including: (1) Familiarization, (2) Generating the initial codes, (3) Searching for themes, (4) Reviewing the themes, (5) Defining and naming the themes and (6) Producing the Report as defined in (Braun, Clarke, Hayfield, & Terry, 2018). During this process, themes emerge from the literature that are related to the state of the art.

After the thematic coding, we applied a topic modelling analysis using a Latent Dirichlet Allocation (LDA). The LDA method identifies topics that best describe a set of documents or articles.

3.4.1 Thematic coding

Thematic coding was adopted to get a baseline understanding of the state of the art in the information technologies for protection of urban space. The list of themes is partially based on the work made in 2004 by R. Popp et al. in (Popp, Armour, Numrych, & others, 2004). This SLR, improved the list of codes in order to present an updated version of technologies for the protection of public spaces. The selected set of articles obtained by the article search were each individually analyzed, labeled and the most important parts were subtracted and stored in an overview with the emerging theme that arose from the analyzed text. This overview served as a total collection of important parts of analyzed text with their concurrent themes and

articles. The aim of the thematic coding was to code as consistent as possible. A method of iterative checking of the themes was applied to obtain the themes as are shown in table Table 4.

Code	Definition	Source
METH	methods for the risk assessment new data sources	PROPOSAL
PRED	Prediction model for prevention measures	PAPER
ASSES	Modeling for assessment. How is the given model evaluating a state	PAPER
FEAS	Feasibility of the posed technique	PAPER
BPGO	Best practices applied by governmental organizations	PROPOSAL
BPOP	Best practices applied by other parties than governmental organizations	PROPOSAL
TECH	Prevention technologies/tools/designs	PROPOSAL
ARIN	Artificial intelligence (machine learning)	PROPOSAL
LACK	Mention of Lack of addressed attention to prevention practices	PAPER
MATU	Maturity level of the grey articles. Based on the Technology readness level	SITE

Table 4 Table of the emerged themes during coding.

3.4.2 Topic Modeling

A Topic Modelling was executed supported with a thematic coding. A Latent Dirichlet Allocation (LDA) was used to provide emerging themes from the text analyzed for the thematic coding, including knowlegde of the theme codes. For the LDA textmining, first some pre-processing was done according to the standard pre-processing for text-mining. The pre-processing was aimed at improving the results by removing words that are not useful for the results. Specifically: (1) Common English words are removed, (2) Punctuation symbols were removed, (3) all capitals were converted to lower-case and (4) all terms and definitions were standardized in terms of structure.

The Log-likelihood was used to measure the performance of the clustering, according to the state of the art methods of measuring quality (Agrawal, Fu, & Menzies, 2016). In the case of this research, the amount of clusters were determined by starting with the default (k=10) and then clusters were checked on overlap. While there was still overlap, the amount of clusters was decreased until no overlap was present. This resulted in the final amount of clusters.

4 Results

This section elaborates on the results of the analysis of this paper. First, the descriptive statistics of the examined papers are provided. An overview is given concerning the year of publication, type of study, and the venue in which the article was published. Subsequently, the results of the LDA topic modeling are given.

4.1 Data sets and Descriptive Statistics

The white literature included into this research have a range of 16 years. In order to limit the scope of this research, a minimum boundary was set. Literature included into this research, should be published after the year of 2003. An emerging trend line is displayed in Figure 4. On average, more recent literature has been found and included in this research.

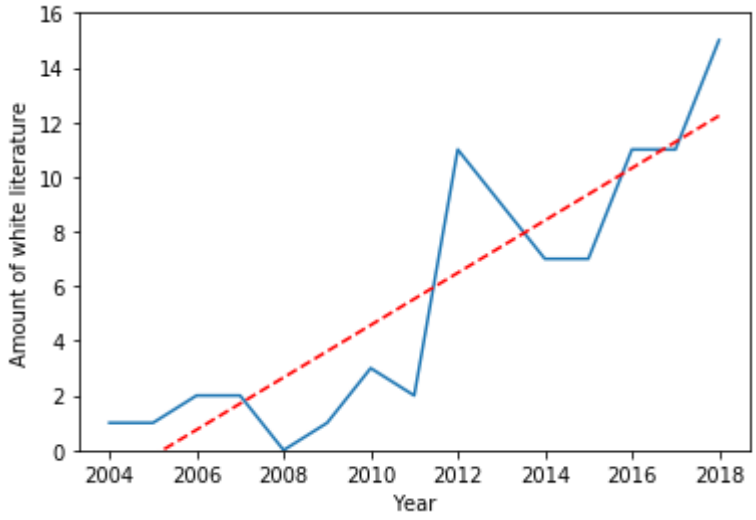


Figure 4 Amount white literature per year of publication.

In Figure 4 the type of studies are displayed. Experimental studies are the most prevalent type of research found within this survey. Literature reviews and case studies cover almost the same amount of white literature in this research. Other consists of empirical and exploratory studies, however these seem to be the least prevalent type of studies within this research.

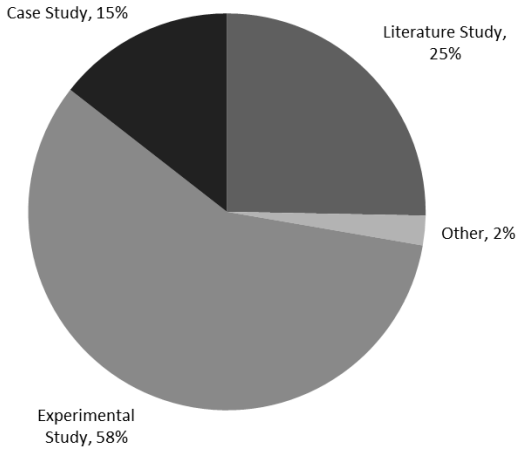


Figure 5 Type of studies within white literature.

Over 50% of the white papers are published as part of journals, as can be seen in Figure 6. Conference papers are also noticeably present in this survey. The third venue, other, consists of books and a magazine.

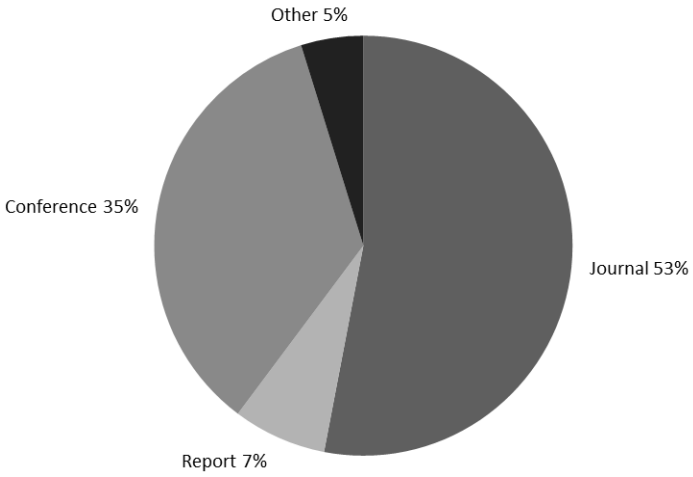


Figure 6 Venues used for publication of white literature.

4.2 Topic modeling

In this paragraph, the results of the topic modeling are discussed. Latent Dirichlet Allocation (LDA) has been applied in order to extract the most relevant themes in the textual data. Before executing the LDA topic modeling, pre-processing needs to be applied to all the text. The pre-processing consists of: (1) removing all punctuation marks and numbers; (2) standardizing terms and definitions structure wise; (3) converting all letters to lower case; (4) removing common stop words for English grammar and syntax.

After the application of the pre-processing, the LDA method for visualizing and interpreting topics was applied. The method used is called LDAvis (Sievert & Shirley, 2014) and is based on the work of Chuang, Manning, and Heer (2012). With the use of the LDAvis, diagrams are plotted. Each circle represents a topic, together with its prevalence. If circles are overlapping each other, means that the topics have common terms. These circles can be found on the left. On the right side, the top-30 most relevant terms are displayed for every topic. The λ slider provides the opportunity for ranking the terms according to term relevance. The range of the slider goes from 0.0 to 1.0. If the slider is close or equal to 0.0, terms be highlighted which are potentially rare but exclusive terms for the selected topic. In this research, the λ is fixed at 0.8 in order to highlight frequent terms but not exclusively.

To gain more insight in the most frequent terms per topic, a bar chart is created with the topic modeling results. In this chart, ten terms are displayed with their probability. The terms are ranked with their accessory probability. The term with the highest probability is displayed at the top.

In the following, the results from the topic modeling are showed and discussed.

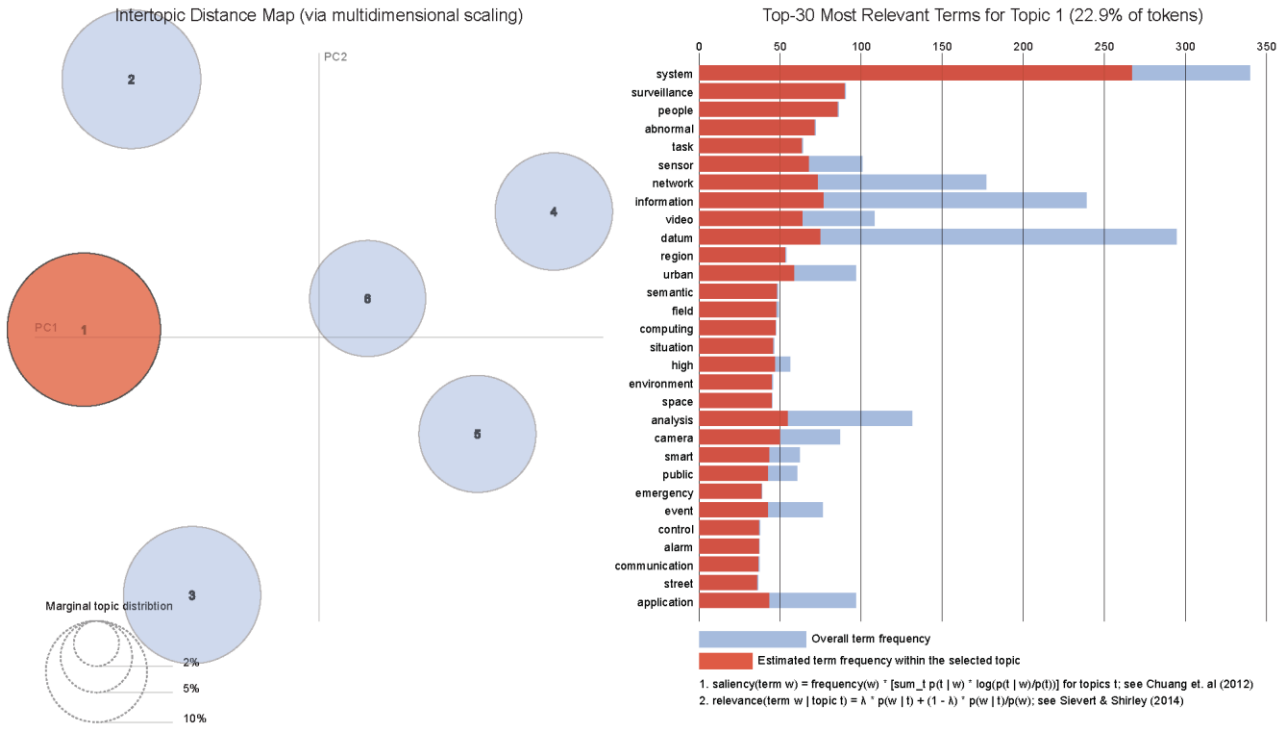


Figure 7 Topic 1 from LDA Topic Modeling.

Terms	**Score**	
System Surveillance	260, 90	Surveillance systems mostly refer to CCTV and security cameras. Moreover, in order to build a surveillance system it is necessary to include components like *Cameras* the main surveillance unit, *Cables* wires to connect cameras with monitors and power adapters, *Power Distribution Block or Power Adapter* power supply unit, *Monitors* screens for surveillance, and *Video recorder (DVR)* hard drive for storage.
Sensor	60	A Sensor is a device that measures physical input from its environment and converts it into data that can be interpreted by either a human or a machine. In the contest of protection of public spaces, Sensors can be used to improve the Surveillance Systems accuracy rather than to be helpful in the context of transforming cities in intelligent environment where if a sensor trigger an exception, an action be taken in order to resolve that event. Sensors can be useful to identifying drivers that run red lights or with high speed, to generating predictive crime maps and risk assessment, to real-time understanding of crowds and their behavior in urban spaces, detect aggressive behavior (Eindhoven municipality is one of the pioneer of this technology).
Urban **Video/Camera** Control	60	Urban Video/Camera Control systems are related to CCTV technologies. In this field we have different types of Cameras like Analog Fixed Cameras, Analog Dome Cameras, Ip Dome Cameras, License Plate Recognition Cameras, Thermal camera (FLIR). Besides, Cameras can be used for a lot of different purposes real-time traffic

	control systems in order to find anomalies, management systems for public infrastructure, identifying all anomalous events occurring on urban streets and dealing with them in real time, optimizing emergency, police and street service response. In order to achieve better results, are now available high performance day/night cameras equipped with IR cut filter system, back light compensation in order to be capable of recording into the dark, interline transfer CCD sensors.

Table 5 Topic analysis results for Topic 1.

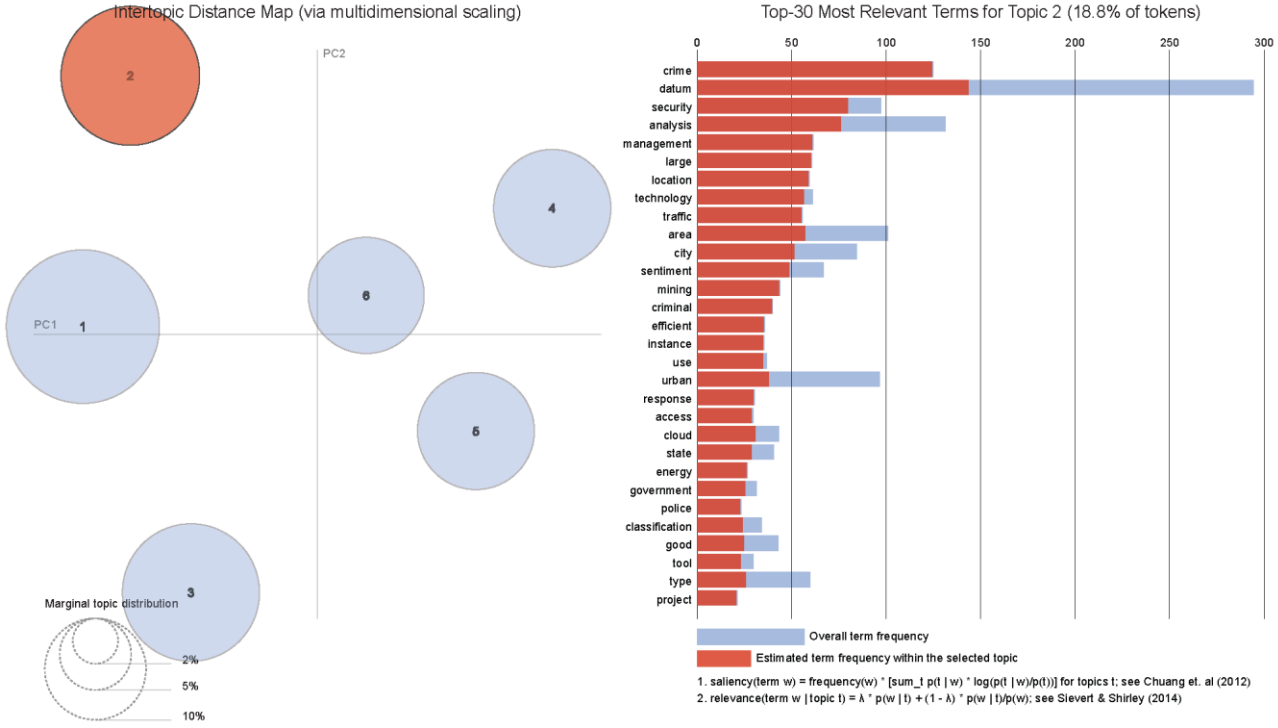


Figure 8 Topic 2 from LDA Topic Modeling.

Terms	**Score**	
Crime Security	130, 70	Security and anticrime policies alone are not enough for responding to all threats and vulnerabilities. Technologies like CCTV and IoT devices can help in improving the security of public spaces. However, we have a new trend from the architectural perspective so called "*Crime Prevention through Environmental Design*" (CPTED). The main idea behind the CPTED strategies relies on the ability to influence offender decisions that precede criminal acts. In this respect, it is important to increase the Natural Surveillance by improving visibility of potential offenders to the general public, Natural Access Control in order to better differentiate among public and private spaces, and Natural Territorial Reinforcement by using buildings, fences, pavement, signs, lighting and landscape to express ownership and define public, semi-public and private space.

Crime Analysis	130, 65	To analyse and prevent crimes in urban areas the best option available is to use the data received from the IoT devices and the surveillance cameras and CCTV in order to build a crime map of the city. From the crime map could be then possible to analyse the factors behind the criminal activities and then address the problems. It is hence important to understand what are the causes that drove a criminal activity and in which location in order to find the right blend of solutions available in the technologies, guidelines and architectural field.
Crime Management	130, 60	Police officers are the main actors in charge of crime management. For this reason it is important to equip the policeman with the right technologies and grant the access to the data that are coming from the technological cities. Connected tablets and smartphones certified by national agencies to provide encrypted communications and in order to share documents in secure and private way. Data harvested from the IoT devices by police can be analyzed to create a picture of crime patterns and trends. By applying predictive analytics and machine learning to big data, police can spot where violent crime may happen next. Facial recognition technology can be implemented into the CCTV and surveillance cameras and could be accessible only by police officers.

Table 6 Topic analysis results for Topic 2.

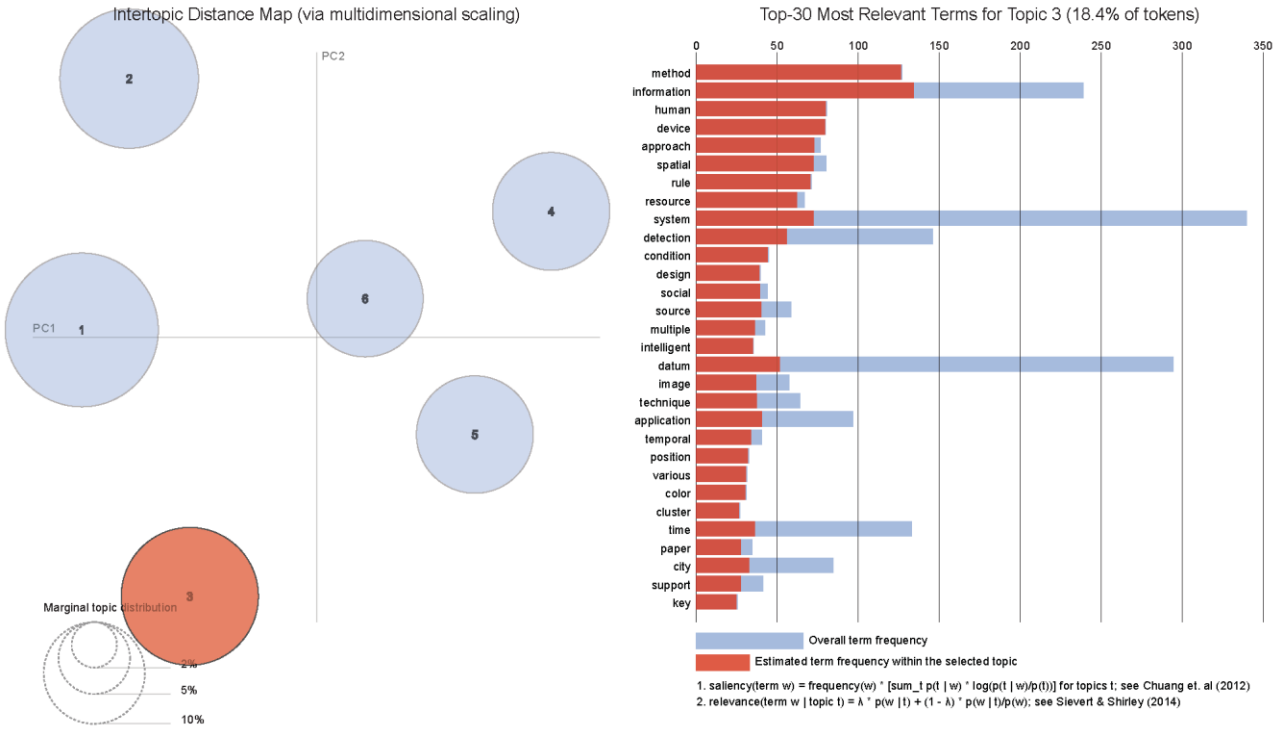


Figure 9 Topic 3 from LDA Topic Modeling.

Terms	Score	
Methods	130	The Methods to guarantee the protection of public spaces are established on the federal and local levels. Authorities should decide and set those indicators for a positive environment with regard to architecture, urban planning and social sphere (Rastyapina & Korosteleva, 2016).
Approach	65	Broader approach is essential to guarantee safety and security in urban spaces. To this respect it is important to have a continuous and systemic process of regulation of problems rather than their eradication or deep transformation. Moreover, it is important to know that municipalities do not have to rely only on traditional security actors, but it is vital to look broader at what are the hazards, decide who might be harmed and how, evaluate the risks, record findings, and review the risk assessment and revise if necessary (Recasens, Cardoso, Castro, & Nobili, 2013) (Roberts, 2018).
Design	40	Different and various are the solution at design level in order to guarantee safer urban spaces. An example could be to plan streets with multiple chicanes, which require vehicles to turn corners and deliberately slows down rather than plan ways in which you can take pedestrians off dangerous corners but still make it convenient for them. Other examples are sidewalks lined with large trees in order to make difficult to the cars to drive on, entirely pedestrianizing popular walking streets could be a solution to keep terror vehicles far from popular areas, ring of steel to protect the most vulnerable urban areas (Mills, 2017) (Economist, 2019).

Table 7 Topic analysis results for Topic 3.

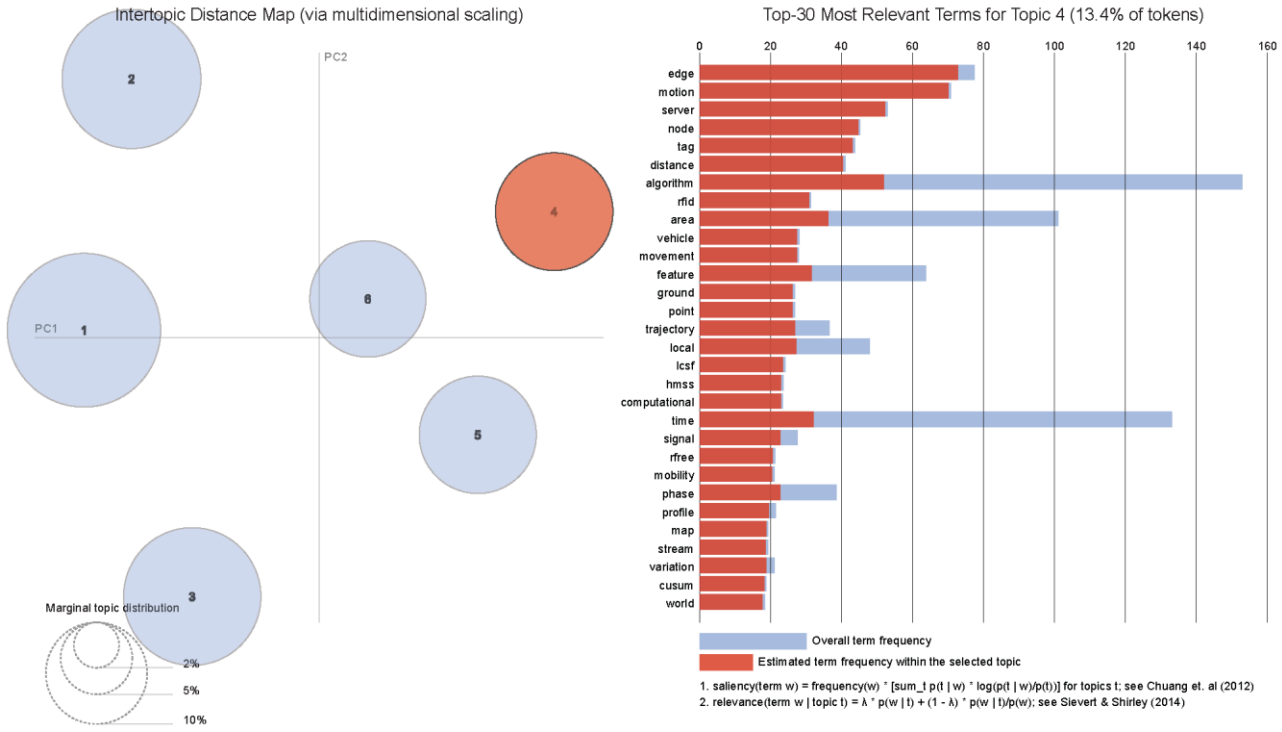


Figure 10 Topic 4 from LDA Topic Modeling.

Terms	Score	
Motion Algorithms	75, 50	Conventional video surveillance systems often rely on human operators for activity monitoring and determining actions to be taken upon incident occurrence. The new era of video surveillance systems provides support to the tedious work of human operators obliged to watch recorded videos in order to find crime proofs. The industry and academics have developed technologies for intelligent surveillance, such as object tracking (Avidan, 2007) (Khan & Gu, 2010), pedestrian detection (Dalal & Triggs, 2005), gait analysis (Wang L. , 2006), vehicle recognition (Wang & Lee, 2007), face and iris recognition (Park & Jain, 2010), and crowd counting (Cong, Gong, Zhu, & Tang, 2009).
Vehicle Movement Trajectory	30, 30, 30	The CCTV and video cameras are nowadays extensively used in order to guarantee safety and security in public spaces. However, in (Life), TNO developed WAMI (Wide Area Motion Imagery) where drones are equipped with high resolution cameras in order to observe a complete city continuously from above. The algorithm proposed by TNO includes object detection, object tracking, tracking repair, and track analytics. WAMI can be used by analyst in to study the behavior of people and vehicles. In (Mehboob, Abbas, Rauf, Khan, & Jiang, 2019) they propose a video visualization system for traffic surveillance. Based on glyph the

	tool can be utilized for road surveillance videos to monitor live road traffic on the highways.

Table 8 Topic analysis results for Topic 4.

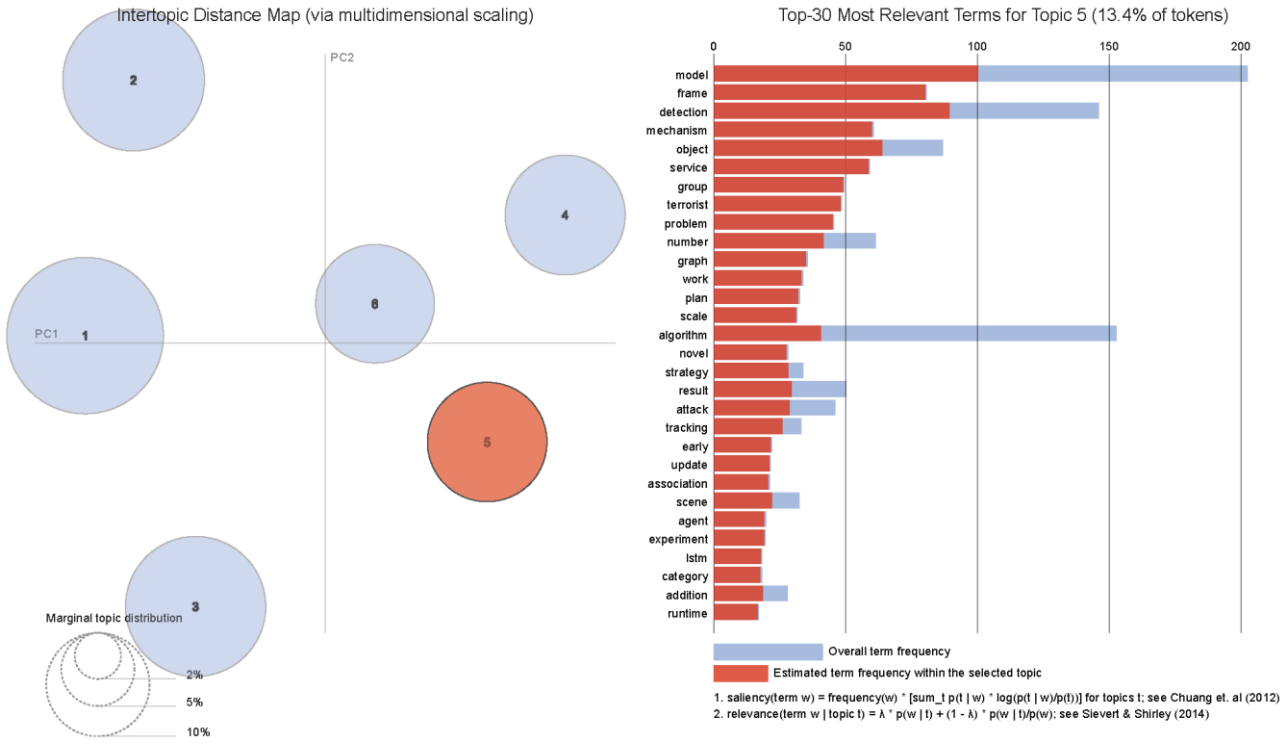


Figure 11 Topic 5 from LDA Topic Modeling.

Terms	**Score**	
Object Detection	60, 90	We can state that for object detection we can use the same technology presented in the other tables from the other topics (motion algorithms, AI, IoT devices).
Work Plan	40, 40	In Table 7 we already discussed methods and approaches that could be taken in order to guarantee protection of public spaces. In (COMMISSION, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Action Plan to support the protection of public spaces, 2017) and in (COMMISSION, SECURITY UNION: PROTECTING PUBLIC SPACES EU MAYORS' CONFERENCE: ``BUILDING URBAN DEFENCES AGAINST TERRORISM'', 2018) some guideline from the European Commission.
Strategy	40	In Table 7 we already discussed methods and approaches that could be taken in order to guarantee protection of public spaces.

Table 9 Topic analysis results for Topic 5.

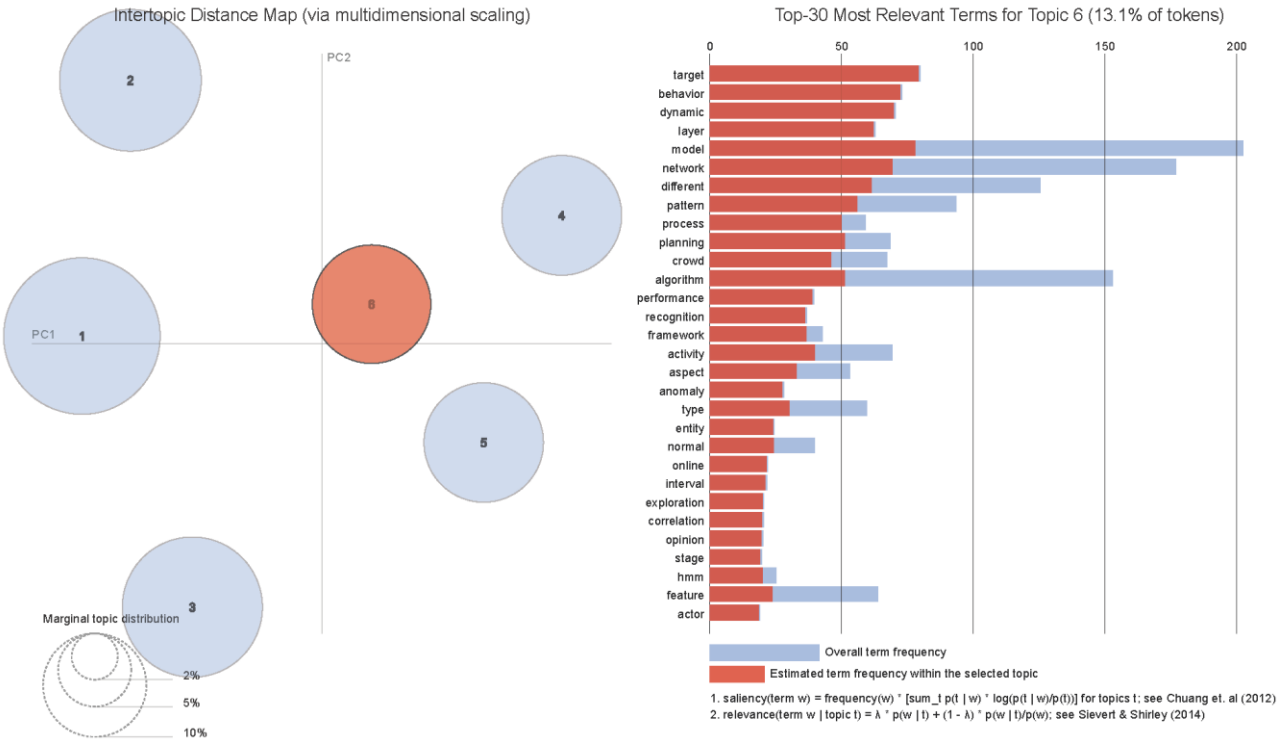


Figure 12 Topic 6 from LDA Topic Modelling.

Terms	**Score**	
Recognition	50	Latest CCTV are equipped with AI in order to recognize different type of objects and scenarios. Hikvision, one of the main supplier of video surveillance products and solutions, in 2017 lunched the first 'Deep Learning' embedded in a Network Video Recorder (NVR) (Hikvision, 2017). The technology presented by Hickvision performs different types of recognitions: *Facial Recognition*, *People counting*, and *Management of vehicles*. Same technology has been implemented also by Huawei and Gigabyte companies and the related products are already available for the market directly from the Huawei webpage[2] and the Gigabyte store[3].
Crowd Behavior	50, 70	Crowd Behavior can be easily addressed by artificial intelligence technology implemented in CCTV and urban cameras. In order to have a wide overview of the city is possible to implement a network composed of AI cameras, IoT devices, and analysis systems so to have a picture about the security state of any urban areas analyzing the data collected from all the different devices at runtime. Moreover, AI itself is already able to detect crowd behavior and anomalies and can be implemented in drones and CCTV, an example

[2] https://e.huawei.com/en/products/intelligent-video-surveillance/cameras/software-defined-camera/x3221-c
[3] https://www.gigabyte.com/Solutions/AI-AIoT/intelligent-video

		of this technology nowadays available are described in (Borja-Borja, Saval-Calvo, & Azorin-Lopez, 2017) (Vincent, Drones taught to spot violent behavior in crowds using AI, 2018) (Singh, Patil, & Omkar, 2018) (Vincent, Artificial Intelligence Is Going To Supercharge Surveillance, 2018) and are available in ICrealtime webpage[4] and in Boulderai webpage[5].
Anomaly detection	40	As for Crowd Behavior, we can use same methods and techniques described also for Anomaly Detection.

Table 10 Topic analysis results for Topic 6.

[4] https://store.icrealtime.com/cameras
[5] https://www.boulderai.com/our-hardware/

5 SLR Conclusions and Discussion

The systematic literature review on best practices and technologies for the protection of public and urban spaces presented here, aims at building an overview of what are the new ``trends'' for the protection of public spaces against terroristic attacks and in order to detect anomalies, prevent crimes and generally how to build safer cities for citizens. First, we collected papers from different online sources both from the academic field and from website and blogs. Once the dataset was completely setup and organized, we started with the coding phase. During the coding phase we manually gave a code to each of the paper in order to categorize them. The codes we used are listed in Table 4. Once all documents from the dataset had been categorized, we applied LDA Topic Modelling on the whole dataset to extract the most relevant themes and compare the results with the codes used for our categorization. In this regards we can assert that exists a concrete overlap among the defined codes and the topic modelling. Indeed, Table 5 presents a list of technologies (**TECH**) used in urban spaces to guarantee safety and security. In Table 6 are discussed techniques to assess and prevent crimes (**ASSES**) which range from how to prevent crimes, how to analyzer those urban areas more subject to criminal events, and how to deal and manage where criminal event are more frequent. In Table 7 our topic modelling analysis grouped the best practices (**BPGO**, **BPOP**) that can be used both at municipal or government level in order to improve the safety and security of urban spaces. In this topic are listed methods, approach and new architectural design technique in order to improve the environment at structural engineering level, a way to rethink our cities and design new spaces and new urban areas that can be considered secure against criminal activities by design. Continuing with our topic modelling analysis results, in Table 8 are listed methods and prediction techniques that can be used to have an additional level of security in urban areas. Finally, in Table 10 are presented techniques that are using Artificial Intelligence algorithms (**ARIN**) in order to enhance the capacities of CCTV, drones, and surveillance cameras.

Considering all our analysis we can finally build a response for our main research question:

"***What are the best practices and technologies, nowadays available, for the protection of urban areas?***"

Finding: there is no one single bullet solution available, conversely, multiple methods and techniques can be put in place to guarantee safety and security in public spaces. The techniques range from architectural design in order to rethink the design of public spaces keeping security into account in continuity to emerging technologies such as AI and predictive surveillance. Moreover, whenever new technologies can appear expensive in cost and questionable in privacy or could be difficult to rethink and re-project public spaces, is always possible to build action plan in order to mitigate, prevent and manage crime events.

6 SLR Limitations and Threats to Validity

Several scope and applicability limitations of our results emerged during our study as well as several threats to the validity of our results. This section provides an outline of both.

First, technologies such as face-recognition technology, event prediction based on human-observation data, crowd behavior, vehicle movement trajectory recognition and more in general AI-based analysis and synthesis information systems are predominant in our sample but pose a huge concern about personal privacy. Threats to privacy revealed by our analysis include: *Lack of Transparency* where people are not aware or did not give the consent to the collection of personal data in public spaces; *Misuse* the images retrieved can be used for different purposes; *Accuracy* could happen to have false-positive matches; human-centered *Automated Decision making* where technology can influence the decision of investigators. The debate about the use of AI in public spaces is in its beginnings and may be the most predominant factor in correlation with the disruptive improvements of AI technology. Our systematic literature review presents the possibility to re-think and re-design AI-based systems with respect to public spaces, their restrictions and features from the architectural level to increase safety and security in public spaces. Lastly, from our SLR we infer the possibility to build best practices and outline action plans to prevent, manage and and analyze crime scenarios and terroristic events.

With respect to the above approaches, this SLR does not strive for a final silver-bullet solution. Conversely, our work gives an overview of the different approaches available in the scientific and non-scientific online literature in order to help municipalities, governmental and non-governmental organizations in defining the best approach as possible for the protection of urban areas against crimes and terroristic attacks.

7 Best practices from Cities and LEAs

This chapter presents and analyzes the outcomes of a survey issued to organizations and networks like EFUS and ENLETS. These best practices that are harvested supplement those that have been extracted in section 2 from the structured literature review.

7.1 Approach and methodology

On the basis of the executed vulnerability assessments and their outcomes, relevant mitigating technological solutions will be selected and will be field-tested from a proof of concept perspective while also encompassing the exchange of best practices and lessons learned.

A questionnaire aiming at local government and LEAs will assist the project in sorting the best applicable technological solutions for demonstration in each EU city participating in PRoTECT, regarding the security of public spaces. The answers from the questionnaire will be valuable in the understanding of each city's specific needs and expectations from the technological solutions, which will contribute towards their higher relevance on the best interest of the stakeholders.

The survey was focused on current solutions, novel solutions of tomorrow, and solutions in the far future for the protection of public spaces, which are implemented or tested in the security domain of local governments and LEAs. The survey was performed using a questionnaire distributed in the ENLETS and the EFUS network and among the five PRoTECT cities (Vilnius, Eindhoven, Malaga, Brasov and Larissa).

7.2 Survey Questionnaire

The best practices questionnaire that was send to local governments and LEAs was entered in a Google Forms environment and electronically send to the ENLETS and EFUS network or published on their respective forums.

The questionnaire consist of the following 7 questions:

Question 1:

What type of organization are you part of:

- Local government ☐
- Law Enforcement Agency ☐
- Research/educational Institute ☐
- Business ☐
- Emergency Response services ☐
- Other: _____

Question 2:

Your position in the organisation:

- Policy maker/advisor ☐
- Administrative ☐
- Field agent ☐
- Researcher ☐
- Other: _____

Question 3:

For which of the following types of attack would you be more interested in seeing the application of a security technological solution in your city? (Rank them from 1-highest to 5-lowest) :

- ***Firearms attack (automatic firearms)*** - e.g. terrorist attacking crowd of visitors in areas of large crowd density with automatic weapons. ☐
- ***Sharp object attacks (mainly knife***) - e.g. random terrorist/criminal acts, or theft. ☐
- ***Vehicle attacks*** – e.g. a vehicle driven into the crowd of visitors at an open space. ☐
- ***IED (explosives)*** – e.g. attacks with explosives against areas with high crowd density. ☐
- ***VBIED (explosives concealed inside a vehicle)*** ☐

Question 4:

The list below consists of different categories regarding the detection, deterrence, prevention and response against terrorist attacks in public spaces. On the basis of aforementioned *types of attack* please rank the following 4 identified technological solution categories (1 = low importance; 5 = high importance):

- **ICT tools (Information and Communication Technology), IoT (Internet of Things)** (communication platforms, integration hubs, open source intelligence, sentiment analysis, social media, discussion fora, etc) ☐
- **Sensor Detection Technology** (including video/sound surveillance, wireless sensor networks, RFID, wearable sensors, etc) and **Actuator** (sirens, anti-drone systems, directed-energy weapons, etc) ☐
- **Social Engineering**: in the context of public spaces, pertains to psychological manipulation of people into performing particular behavior in public spaces. (nudging, citizens participation, community building, etc) ☐
- **Knowledge and training:** (develop expert knowledge on anti-terrorism and train/simulate/serious game/exercise ☐
- **Electrical and Physical Barriers and Access Management**. (automatic identification, risk analysis (vulnerabilities), geofencing, etc). For the purpose of: crowd management, event management, stopping moving vehicles/drones, etc ☐

Question 5:

Are there any specific criteria that would be of support to you in potentially selecting a solution for deployment against any of the attack types indicated in question 2? Please check any of the following indicative criteria or add additional:

- **Size –** Dimensions of underlying filed equipment ☐
- **Weight –** Weight of portable equipment ☐
- **Cost -** Indicative cost for a potential deployment in a given operational set up ☐
- **Scalability** - the potential of the system to accommodate a large number of external sources, without degrading performance ☐
- **Portability** - Capacity to deploy a system in a number of different operational environments without significant reconfiguration ☐
- **Reliability**: - Provide for a continuously operational system which is available across a range of different field environments ☐
- **Modularity** – Capacity for functionality to be implemented within a particular operational environment without deploying the whole system ☐
- **Interoperability** - exchange of information with existing/other external systems ☐
- **Please add new ones:** …….

Question 6:

Have you implemented, developed and/or tested any type of solution/best practice to protect public spaces against terrorist threats in the past or plan to implement in the near future?

- Yes (continue with question 5)
- No

Question 7:

Please describe solutions/best practice you have implemented, developed and/or tested in the past for the overall security of public spaces in your city (terrorist attack and criminality mitigation) or are thinking about doing so (max 3):

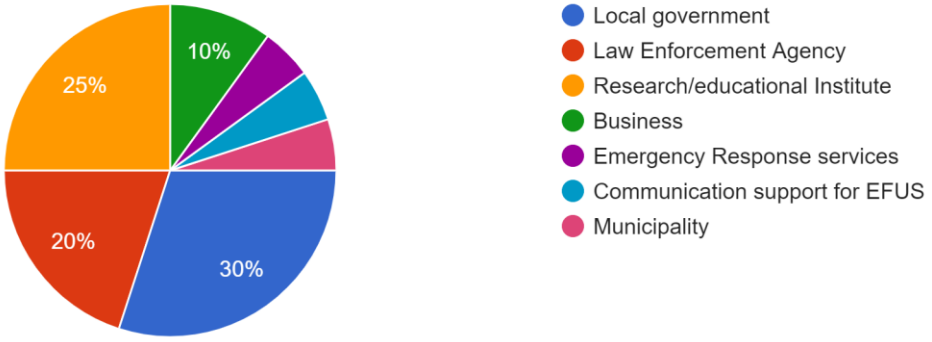
Solution name	
Short description (Please add information about the purpose and function of the solution)	
Relevant threat type	- Firearms attack (automatic firearms) ☐ - Sharp object attacks (mainly knife) ☐ - Vehicle attacks ☐ - IED (explosives) ☐ - VBIED (explosives concealed inside a vehicle) ☐ - Other: ……..
Solution category	- ICT and IoT platforms ☐ - Sensor Detection and Actuator Technology ☐ - Social Engineering ☐ - Knowledge and training ☐ - Electrical and Physical Barriers and Access Mgt. ☐ - Other: ……
Status of the solution	- Described Idea ☐ - Research project ☐ - Pilot/field test ☐ - Product ☐ - Other: ……
Owner name (Organisation)	
Contact info	- Contact person - Email - website
Other relevant information	

7.3 Results

Based on the 20 received filled in questionnaires the results are shown in the diagrams below:

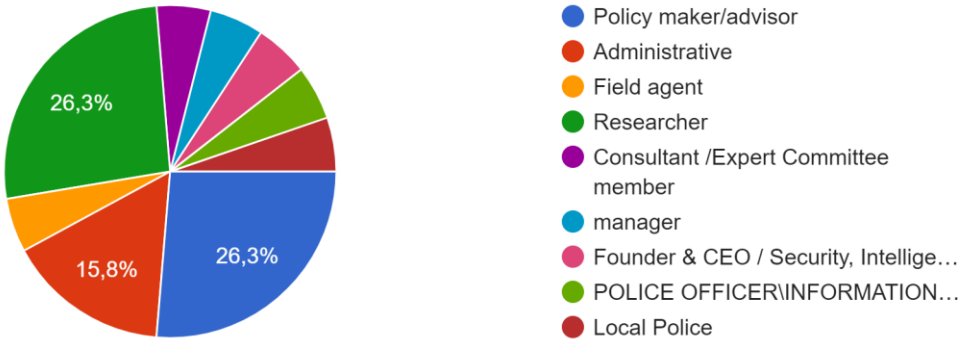
Question 1:

20 antwoorden



Question 2:

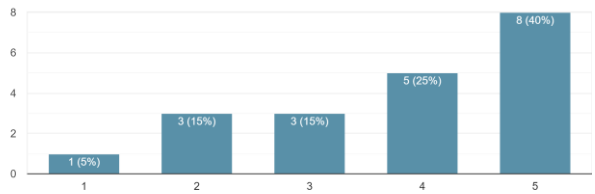
19 antwoorden



Question 3:

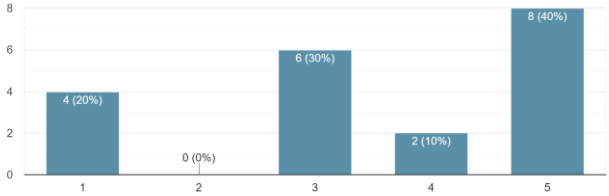
Firearms attack (automatic firearms) - e.g. terrorist attacking crowd of visitors in areas of large crowd density with automatic weapons.

20 antwoorden

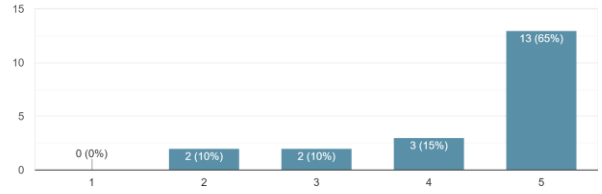


Sharp object attacks (mainly knife) - e.g. random terrorist/criminal acts, or theft

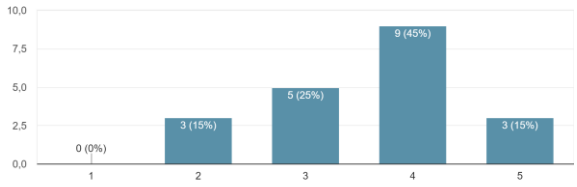
20 antwoorden



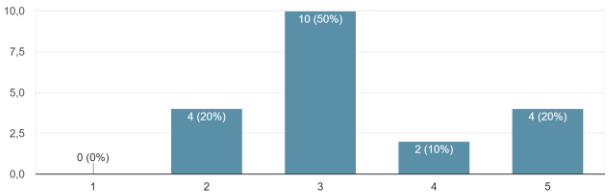
Vehicle attacks – e.g. a vehicle driven into the crowd of visitors at an open space
20 antwoorden



IED (explosives) – e.g. attacks with explosives against areas with high crowd density
20 antwoorden

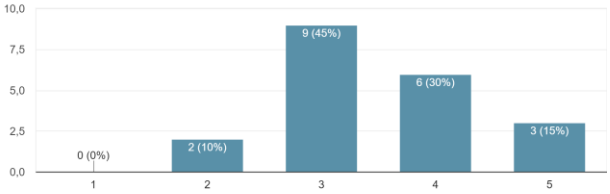


VBIED (explosives concealed inside a vehicle)
20 antwoorden

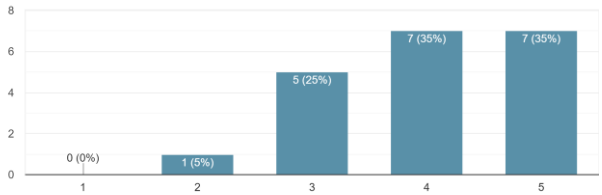


Question 4:

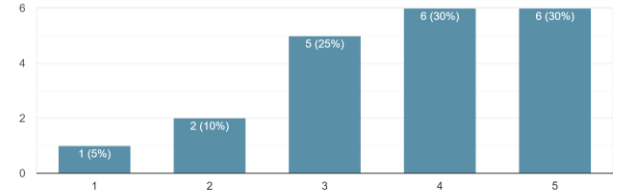
ICT tools (Information and Communication Technology), IoT (Internet of Things) (communication platforms, inte...s, social media, discussion fora, etc)
20 antwoorden



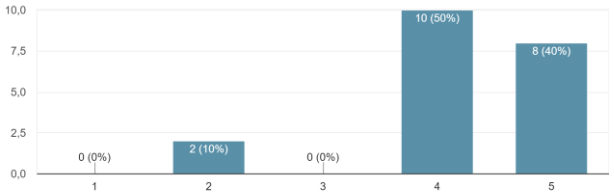
Sensor Detection Technology (including video/sound surveillance, wireless sensor networks, RFID, wearable senso...stems, directed-energy weapons, etc)
20 antwoorden

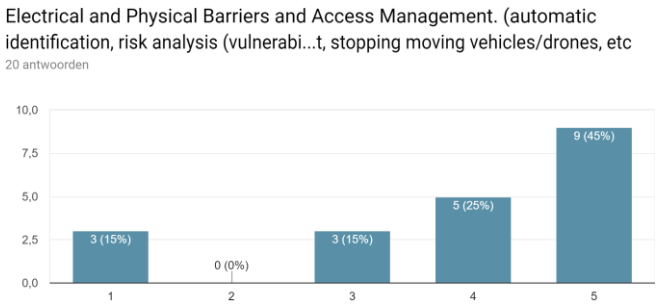


Social Engineering: in the context of public spaces, pertains to psychological manipulation of people i...articipation, community building, etc)
20 antwoorden

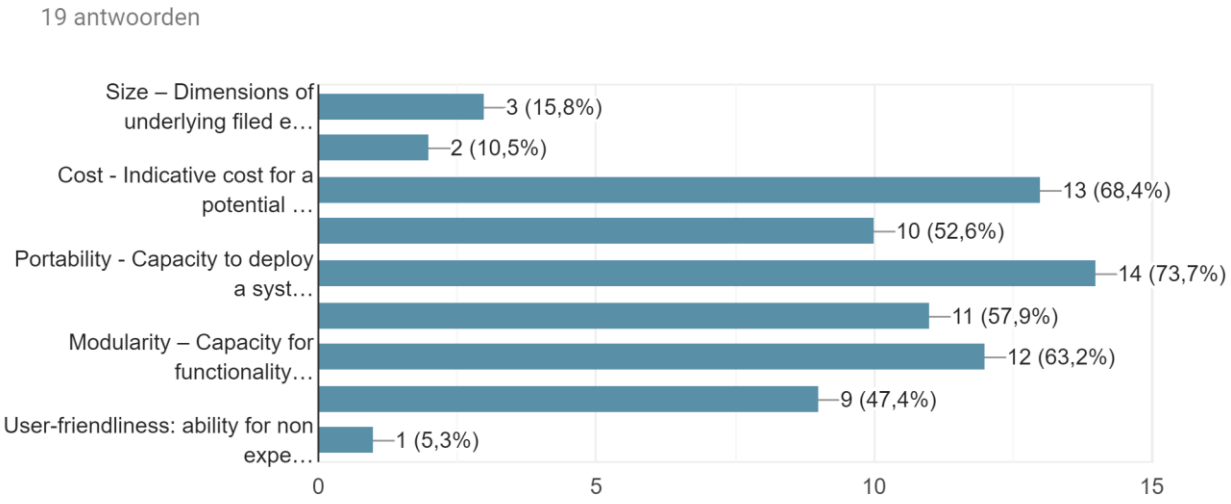


Knowledge and training: (develop expert knowledge on anti-terrorism and train/simulate/serious game/exercise)
20 antwoorden

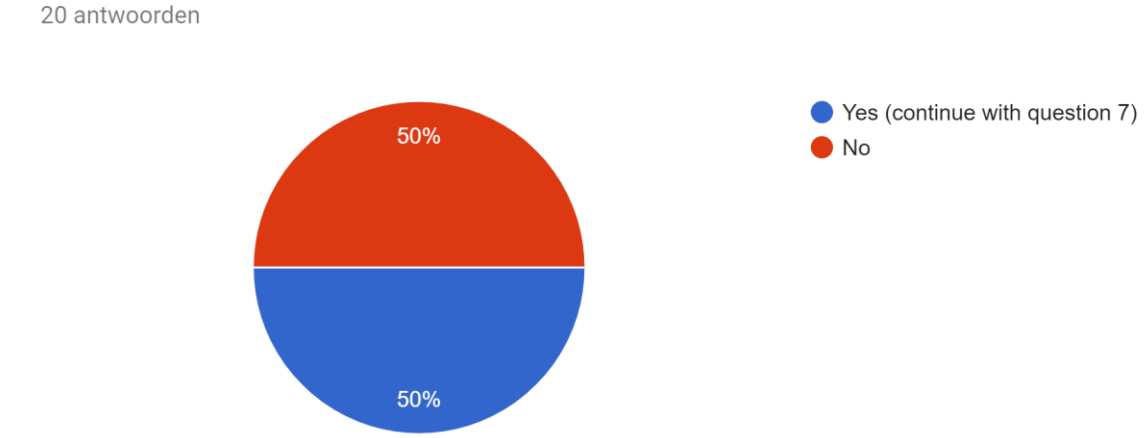




Question 5:



Question 6:



Question 7:

This question had a maximum of 3 tables for each best practice solution/product/project that could be filled in. In total there are 19 responses:

Solution names (or descriptions):

1. Road closing with buses and trucks
2. In Edinburgh theocal authority have developed flexible hostile vehicle deterrent
3. LBASense
4. buying tested mobile barriers (Indutainer, Pitagone) and using them at the perimeter of events in public space to either block access or to slow down approaching vehicles, depending on how the barriers are deployed
5. Hostile Vehicle Mitigation - A series of IWA 14 rated, rise and fall bollards have been installed around the pedestrianised area of Leeds City Centre.
6. Vehicle mitigation barriers/bollards
7. Video surveillance system
8. ECOPOL, full spectrum situational awareness
9. SAFECITY
10. Asgard - Tool set for the extraction, fusion, exchange and analysis of Big Data, including cyber-offense data for forensic investigation
11. We are planning to buy a few things from another company or companies, also to test them
12. Stay Safe Training. A number of awareness raising presentations to council employees, partner agencies, public bodies. Over 200 sessions have been delivered to date.
13. Video surveillance system
14. P-REACT
15. STEPWISE - Platform aiming to enable the rapid creation of Virtual Reality mock-ups of real-world spaces and buildings where security and crisis plans can be devised and assessed against a wide variety of threat scenarios.
16. We are analysing perimeters trying to implement intelligent street furniture and landscape design (Planters, ditches, Banks etc) as a means to mitigate vehicle borne threats. This will be mixed with "normal" bollards where needed
17. Emergency Incident and Business Continuity Workshops. - Parners invited to attend a scenario led exercise in order to assess the validity of their own plans.
18. Vehicle anti-attack system
19. media4sec

Respective Solution owner:

1. Riga municipal police
2. City of Edinburgh Council
3. DFRC
4. Department of Security and Public Order Munich
5. Leeds City Council
6. City of The Hague
7. IDIS Solution Suite
8. LT Startcom
9. ISDEFE (Coordinator)
10. EU Research Project
11. Department of security and public order, Munich
12. Leeds City Council
13. AVIGILION

14. Vicomtech (Coordinator)
15. EU Research Project
16. Department of security and public order Munich
17. Leeds City Council
18. GRUPO INESUR
19. WARWICK University (Coordinator)

Solution category:

- ICT and IoT platforms : 6
- Sensor Detection and Actuator Technology : 4
- Social Engineering : 4
- Knowledge and training : 5
- Electrical and Physical Barriers and Access Mgt. : 6
- Other: …… : 1

8 Survey related EU projects

This chapter outlines the outcome of the detailed survey towards related EU- and national projects that address (elements of) the PRoTECT project.

8.1 Approach

The survey on European Union member states Projects that address elements of the PRoTECT project was conducted as a need to document innovative solutions (EU-based) originated from EU research projects in the security domain. The survey was focused on current solutions, novel solutions of tomorrow, and solutions in the far future for the protection of public spaces, which are originated from EU research projects in the security domain. The survey was performed using two methods: a questionnaire distributed in the ENLETS network and open source research performed by IGPR project team.

8.2 Relevant EU Funds and related projects

NR.	Financing	Project name	Type of technology	APLICABILITY /SCENARIO
1.	H2020	FORENSOR FOREnsic evidence gathering autonomous sensor project reference no. GA 653355	Sensors : EVIDENCE GATHERING SENSOR with ultra-sensitive camera and built-in intelligence.	After attack Forensics applications for LEAs. Operate at remote locations, automatically identify pre-defined criminal events, and alert LEAs in real time while providing and storing the relevant video, location and timing evidence
2.	H2020	BigClouT Distributed Intelligence for Smarter Cities project reference no. GA 723139	IoT: Cloud and big data capabilities, intelligence gathering	Provide cities with the analytic capability needed to exploit the Big Data coming from IoT devices, open data sources, social networks and mobile applications
3.	H2020	City Risk Avoiding and mitigating safety risks in urban environments project reference no. GA 653747	ICT: Web and social media platform for actively contributing citizens	Before, during, after attack Framework among authorities and citizens through mobile applications that will allow in a collaboratively way to prevent or mitigate the impact of crime incidents or other security threats
4.	H2020	SURVEIRON Advanced surveillance system for the protection of urban soft targets and urban critical infrastructures project reference no. GA 711264	ICT, Sensors: Fleet of intelligent robots/aerial vehicles UAVs	During and after attack; Surveillance and detection technologies
5.	H2020	SPIDERS Synthetic aPerture Interferometric raDiometer for sEcurity in cRitical	ICT, Sensors: Passive scanning system, interferometric radiometer	3D scanning system of walking people and detection of hidden objects and material

NR.	Financing	Project name	Type of technology	APLICABILITY /SCENARIO
		infraStructures project reference no. GA 674274		
6.	H2020	ChemSniff Chemical sniffer device for multi-mode analysis of threat compounds project reference no. GA 674716	Sensors: ion trap (LIT) mass spectrometer (MS) operating in a non-scanning mode	Real-time detection of chemical compounds
7.	H2020	BIO-AX A novel wearable, cost-effective and non-invasive biometric body worn video solution for accurate and high throughput screening of people, bags and vehicles project reference no. GA 719806	ICT, Sensors: body worn video solution (ecosystem)	Secure evidential video gathering and live stream to command centre
8.	H2020	INGENIOUS The First Responder (FR) of the Future: a Next Generation Integrated Toolkit (NGIT) for Collaborative Response, increasing protection and augmenting operational capacity project reference no. GA 833435	ICT, Sensors, Actuators : Next Generation Integrated Toolkit (NGIT) for Collaborative Response	Information sharing and communications between teams and with victims
9.	H2020	EXERTER Security of Exlosives pan-European Specialists Network project reference no. GA 786805	Method: Network with Explosives Specialists	Research and innovation in Security of Explosives
10.	H2020	I-LEAD Innovation - Law Enforcement Agency's dialogue project reference no. GA 740685	Method: Defining needs for innovation	Practitioner groups and advise the Member States regarding Public Procurement of Innovation Technologies
11.	H2020	ENTRAP Enhanced Neutralisation of explosive Threats Reaching Across the Plot project reference no. GA 730560	ICT: Tools for Morphological analysis, attack-defence trees, Bow-tie diagrams and wargaming	Before attack countering present, emerging and future explosive threats
12.	H2020	IN-PREP Crossing New Frontiers in Disaster Preparedness project reference no. GA 740627	ICT, Method: Framework for improving and planning of joint interventions	Before attack Improving the joint capacity to respond
13.	H2020	ASGARD Analysis System for Gathered Raw Data project reference no. GA700381	ICT : Solutions for processing of seized data, availability of massive amounts of data and big data	Before attack Forensics, Intelligence and Foresight (Intelligence led prevention and anticipation)
14.	H2020	CYBER-TRUST Advanced Cyber-Threat Intelligence, Detection and mitigation Platform for Trusted Internet of Things project reference no. GA 786698	ICT - IoT: Cyber-Threat Intelligence, Detection and mitigation Platform for Trusted Internet of Things	Capture different phases of emerging attacks by cyber-criminals, before and after attack

NR.	Financing	Project name	Type of technology	APLICABILITY /SCENARIO
15.	H2020	ASTRID Adressing ThReats for virtualized services project reference no. GA 786922	ICT : Technology for planning cloud applications and Network Function Virtualisation	Unified access and encryption management, correlation of events and information among different services/applications, support for legal interception and forensics investigation
16.	H2020	TENSOR Retrieval and analysis of heterogenous online content for terrorist activity recognition project reference no. GA 700024	ICT : Terrorism intelligence platform, tools for efficient and effective searching, crawling, monitoring and gathering online terrorist-generated content from the Surface and the Dark Web	Recognition, retrieval and analysis of online content for terrorist activity
17.	H2020	PROPHETS Preventing Radicalisation Online through the Proliferation of Harmonised ToolkitS project reference no. GA 786894	Method : Setting up a security model for preventing radicalisation online (interplay of human factors and cyber ecosystem)	Identification, investigations and response to security threats, communication strategy
18.	H2020	EVAGUIDE Security management Platform for enhanced situation awareness and real-time adaptive evacuation strategies for large venues for sports and entertainment project reference no. GA831154	ICT: Security Management Platform	Complex evacuation processes for large facility
19.	H2020	beAWARE Integrated solution to support forecasting, early warnings, transmission and routing of emergency data, aggregated analysis of multimodal data, and management tha coordination between the first responders and the authorities project reference no. GA 700475	ICT : Integrated solution to support forecasting, early warnings, transmission and routing of emergency data, aggregated analysis of multimodal data, and management tha coordination between the first responders and the authorities	Provide support in all the phases of an emergency incident
20.	H2020	MAGNETO Multimedia Analysis and correlation enGine for orgaNised crimE prevenTion and investigatiOn project reference no. GA 786629	ICT : Sophisticated knowledge representation, advanced semantic reasoning and augmented intelligence, well integrated in a common, modular platform with open interfaces	Crime analysis, prevention and investigation capabilities,
21.	H2020	MEDEA Mediterranean practitioners' network capacity building for effective response to emerging security challenges project reference no. GA 787111	Method: Regional Networks of practitioners and other security related actors in the Mediterranean and the Black Sea region.	Research, Development and Innovation (RDI) initiatives, within Thematic Communities of Practitioners (TCP): Managing of migration flows and asylum seekers, Border management and surveillance, Fight against cross border organized crime and terrorism, Natural hazards and technological accidents.

NR.	Financing	Project name	Type of technology	APLICABILITY /SCENARIO
22.	H2020	CITYCOP Citizen Interaction Technologies Yield Community Policing project reference no. GA 653811	ICT : 4 tools: a portal, a central back-end system, mobile app, a social media infrastructure	Training game for LEA officers based on scenario building and reaction and Privacy-by-design methodology
23.	H2020	TRILLION TRusted, CItizen - LEA colLaboratIon over sOcial Networks project reference no. GA 653256	ICT : Multiple channels for incident reporting and interaction	Facilitating information sharing and effective collaboration between citizens and LEAs
24.	H2020	AirBrush A fast non-intrusive vapour detection system that rapidly identifies explosives in public areas project reference no. GA 811977	sensors: Non-intrusive vapour detection system - Ion Mobility Spectrometry (IMS) sensor	Optimize the AirBrush design and validate its performance through pilot test with NCTV at Schiphol Airport
25.	H2020	AUGGMED Automated Serious Game Scenario Generator for Mixed Reality Training project reference no. GA 653590	METHOD, ICT: a serious game platform	Training game for first responders
26.	H2020	SURVANT SURveillance Video Archives iNvestigation assisTant project reference no. GA 720417	ICT: Innovative system that will collect the relevant videos from heterogeneous repositories	capabilities for accurate search queries and results using advanced visualization tools
27.	H2020	VICTORIA Video analysis for Investigation of Criminal and TerrORIst Activities project reference no. GA 740754	ICT: Develop a TRL-6 video analysis technology, Create a business model and ecosystem, Train LEA investigators	Video analysis for Investigation of Criminal and TerrORIst Activities
28.	H2020	STAIR4SECURITY STANDARDS, INNOVATION AND RESEARCH FOR SECURITY project reference no. GA 853853	METHOD: A collaborative platform as single entry point of information on the security sector coming mostly from research activities	An overview of current and new projects: national European or International level, ensure more coordination between all stakeholders,
29.	H2020	RED-Alert Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing project reference no. GA 740688	ICT: Data mining and predictive analytics tools: novel natural language processing, semantic media analysis social network analysis (SNA), Complex Event Processing (CEP) and artificial intelligence (AI) technologies	The RED-Alert solution will outperform state-of-the-art solutions in terms of number of languages supported, privacy preserving capabilities, usability, detection performance, real-time capabilities and integration capabilities
30.	H2020	Arcopter The Game Changer Free-wing VTOL Drone for Commercial and Governmental Missions project reference no. GA 816552	Sensors: Drone for Commercial and Governmental Missions (UAV), that combines fully autonomous operation, accurate Vertical Take-Off and Landing (VTOL) and capability to operate in windy conditions, fully autonomous operation carrying a variety of payloads (cameras) based on the customer's needs and application	During the attack and after for providing safety, efficiency for LEA's purposes
31.	H2020	CURSOR Coordinated Use of miniaturized Robotic	ICT, Sensors, Actuators: Miniaturized robotic equipment and advanced	Information and data gathering after attack.

NR.	Financing	Project name	Type of technology	APLICABILITY /SCENARIO
		equipment and advanced Sensors for search and rescue OpeRations project reference no. GA 832790	sensors including Unmanned Aerial Vehicles (UAVs) for command & control, 3D modelling and transportation of disposable miniaturized robots equipped with advanced sensors for the sensitive detection of volatile chemical signatures of human beings	
32.	H2020	DARWIN Expecting the unexpected and know how to respond project reference no. GA 653289	METHOD: European resilience management guideline	Improvement of stakeholders ability to anticipate, monitor, respond, adapt, learn and evolve, and to operate efficiently in the face of crises
33.	FP7-SECURITY	VALCRI Visual Analytics for Sense-making in CRiminal Intelligence analysis project reference no. GA 608142	ICT, Sensors: Information analysis system based on visual analytics, text processing	Before and after attack, advanced query and representation of data capabilities
34.	FP7-SECURITY	DRIVER+ DRiving InnoVation in crisis management for European Resilience project reference no. GA 607798	Method: Portfolio of solutions (online catalogue), Centre of Expertise	Innovative solutions in crisis management and European Network for crisis management innovation
35.	FP7-SECURITY	P-REACT Petty cRiminality diminution through sEarch and Analysis in multi-source video Capturing and archiving plaTform project reference no. GA 607881	Low-cost cameras and smart sensors (video and motion) sensor data (video and motion); Capturing and archiving network/platform that allows the protection of small businesses from petty crimes	Monitoring and recording (data gathering) for the protection of small businesses from petty crimes
36.	FP7-SECURITY	INACHUS Technological and Methodological Solutions for Integrated Wide Area Situation Awareness and Survivor Localisation to Support Search and Rescue Teams project reference no. GA 607522	METHOD, SENSORS, ICT: a. Simulation tools for estimating the locations of survival spaces b. Decision and planning modules for advanced casualty and damage estimation c. Integration of sensors and mobine signals d. A snake robot mechanism (integrated with the sensors) to penetrate inside the rubble e. communication platform f. data analysis techniques and 3-D visualization tool g. System Integration of all the aforementioned software and hardware subcomponents h. Contribution to standards i. Consideration of societal impacts and legal/ethical issuesj. Numerous field and simulated tests properly Appropriate training package and extensive training courses	After attack search and rescue operations
37.	FP7-SECURITY	EXPEDIA EXplosives PrEcursor Defeat by Inhibitor Additives project reference no. GA 604987	METHOD: A European guide for first responders with basic instructions on how to interpret findings on a crime	Increase the security of the citizens in Europe. Increasing the understanding of how terrorist's create

NR.	Financing	Project name	Type of technology	APLICABILITY /SCENARIO
			scene when suspected bomb factories have been encountered.	homemade explosives (HME), what chemicals they start from and where they find them in the open market
38.	ISFP-2017-AG-IBAATLAS	ATLAS 2017 a transnational network of 38 special intervention units from all 28 EU-MS and Iceland, Norway and Switzerland organizing joint trainings and exercises in maritime and urban environment project reference no. GA814730	Method : Joint trainings and exercises in maritime and urban environment	Tactical and technical intervention skills are improved and standardized
39.	ISFP-2017-AG-IBAENLETS	ENLETS ETP project reference no. GA 814756	Method : Network of Law Enforcement agencies	Sharing best practices: exchange knowledge on technology between member states, co creation, enhance cooperation on projects and research
40.	ISFP-2017-AG-IBARAILPOL	RAILPOL project reference no. GA 821848	Method : International association of governmental controlled police organisations	Enhance and intensify international railway police cooperation, to prevent threats, to guarantee the effectiveness of measures against cross-border crime and to be the link between the police and the railway sector
41.	ISFP-2017-AG-PROTECT	BULLSEYE harmonize the different existing procedures and the used equipment in the EU countries to respond to a chemical or a biological terrorist attack project reference no. GA 815220	Method : Cross-sectoral exercise and train the trainer course	Exchange of chemical or a biological terrorist attack knowledge and procedures
42.	ISFP-2017-AG-PROTECT	Pericles preventing vehicle ramming attacks project reference no. GA 815358	Method, Physical: European vulnerability tool Improvement of physical security measures in public spaces	Before a terrorist attack, taking into account aesthetics and the open nature of public spaces in order to minimize the impact on society
43.	ISFP-2017-AG-PROTECT	PACTESUR Protect Allied Cities against TErrorism in Securing Urban aReas project reference no. GA 815091	Method : Well-structured framework defining how cities and local police forces can better protect their vulnerable public spaces	Strengthening cooperation between cities and convergent strategies on urban security
44.	ISFP-2017-AG-PROTECT	MELODY A harmonised CBRN training curriculum for first responders and medical staff project reference no. GA 814803	Method : CBRN training curriculum for first responders and medical staff	Improvement of first responders capabilities
45.	ISFP-2017-AG-PROTECT	XClanLab Application for mobile devices to identify a clandestine laboratory for homemade explosives project reference no. GA 815359	ICT: Application for mobile for Android and IOS devices	Report information and photos from the scene transferred to experts

NR.	Financing	Project name	Type of technology	APLICABILITY /SCENARIO
46.	ISFP-2017-AG-PROTECT	SECUR-CITIES Prévention et sécurité dans les espaces publics des villes européennes project reference no. GA 815391	Method: A transferable model for European cities, regarding new security equipment to better protect potential targets, the need to rethink urban planning and to develop a genuine safety culture	Strengthen the protection measures in the public area by all actors. Develop new local approaches to secure public spaces and develop exchanges of practices on this matter; Test new equipment and technologies to improve public safety.
47.	ISFP-2017-AG-PROTECT	PRINCE Preparedness Response for CBRNE incidents project reference no. GA 815362	Method: Produce a roadmap and recommendations by creating a catalogue of training curricula	Sharing information on CBRN threat and risks, exchange best practices and joint trainings and exercises
48.	ISFP-2017-AG-PROTECT	SafeCi Safer Space for Safer Cities project reference no. GA 814892	Method: Joint workshops and a handbook with recommendations	Enhancing the protection of public spaces and other soft targets
49.	ISFP-2017-AG-PROTECT	SHERPA Shared and coherent European Railway Protection Approach project reference no. GA 815347	Method: Up-to-date knowledge base on threats and countermeasures (both technical and procedural); a coherent approach for risk assessment, risk management, crisis and disaster recovery management; strengthening co-operation among stakeholders through high-level international trainings and other practical tools; outlining needs and requirements	Improving the overall protection level for stations and trains in Europe against terrorist
50.	ISFP-2017-AG-PROTECT	Skyfall LEA training for Counter-UAV Protecting europe against UAV threats project reference no. GA 815244	Method: A matrix how to protect and respond on different types of UAV incidents and a study of all systems currently available, which are suitable for physical drone interception	Improving preparedness and response levels of LEA's
51.	ISFP-2017-AG-PROTECT	CERBERUS The establishment of the Central European Regional Mobile CBRN-E/Dirty Bomb First Responder Unit project reference no. GA 815310	Method : Establishing the Central European Regional Mobile CBRN-E/Dirty Bomb First Responder Unit as unique cross border and cross-sectoral cooperation and coordination mechanism	Improvement of the training facilities
52.	ISFP-2017-AG-PROTECT	DirtyBomb Increased preparedness to CBRN incidents via first responders' joint exercises project reference no. GA 815151	Method: Identification of critical points to be improved and development of training materials for the EU LEAs	Enhance the level of preparedness of first responders
53.	ISFP-2017-AG-PROTECT	STEPWISE A Simulation, Training, and Evaluation Platform for the Protection of Crowded Public Spaces project reference no. GA 815182	Method: Digital models of places and buildings, study of security design, assessing the degree of vulnerability of public spaces	Sharing of knowledge on the protection of public spaces

NR.	Financing	Project name	Type of technology	APLICABILITY /SCENARIO
54.	ISFP-2018-AG-CT-PROTECT	QROC Quick response for Operational Centres project reference no. 861716	Method: Identify needs and best practices regarding new innovative technologies for operational centres to improve public protection	Cross border communication capability between law enforcement National Operational Centres

Table 11 List of EU projects related to the protection of public spaces

9 Overview of technologies

This chapter summarizes the outcomes of the exploration of technologies that mitigate vulnerabilities (associated to threats) for the protection of public spaces as provided by the involved five cities of PRoTECT. The technologies have been explored regarding vulnerabilities that came out of the vulnerability assessments and the specific attack types formulated by the EU VAT. This scoping has made it possible to explore technologies and results in a first list of technologies that not yet include all existing (future) technologies.

The technologies can be used by the 5 beneficiary cities (and in the future all municipalities) to get more understanding of which technologies could aid in protecting public spaces against terrorism. Furthermore, it provides input to decide on qualities, functions and criteria during the other activities of the PRoTECT project. The explored technologies are reported on different aspects, like their functional and non-functional properties, what threat types and threat phases they are applicable to, the use of these technologies and sometimes specific products. The focus is on technology types and not specific products or suppliers. For the purpose of the PRoTECT project, there is a broad need to understand what technologies aid in protecting public spaces. Later on in the project, using an RFI and demonstrations, there will be more focus on actual products or other ideas that could be implemented.

9.1 Approach

To explore and gather relevant technologies that aid in the protection of public spaces against terrorist attacks, different activities have been set out.

First, there has been an analysis of the EU VAT reports of all cities to get an understanding of the needs that resulted from the vulnerabilities. These have been used as context for the researchers and experts and used to relate technologies to specific usage. Second, multiple aspects to report on the technologies have been developed. These aspects consist of a technology description, technology category, threat types, threat phases, technology use (measure type), common criteria and potential products or suppliers. These aspects are based on input from the EU VAT and discussions with the relevant partners on scoping. Third, a first workshop with different experts on technologies that could be of use in the context of protecting public spaces against terrorism was held. This workshop aim was twofold, on the one hand it was to discuss the approach, developed aspects and to see if this could lead to relevant technology results. On the other hand, it was to see if these different experts could provide relevant technologies to include in the list of technologies. Fourth, after a revision of the aspects and scoping, a survey was set out to different experts to provide technologies. Fifth, the technology results have been analysed and categorized according to the five technology categories and been reported on the pre-described aspects. The full list of technologies can be found in appendix IV.

The following paragraphs will describe the analysed needs based on vulnerabilities, the aspects that every technology has been reported on and a summary of the technology results.

9.2 Municipality needs from vulnerability assessments

To have a better understanding of what is needed and what technologies should be explored, there has been an analysis of the EU VAT reports of all 5 cities. This had created some scoping to discuss and explore technologies. The EU VAT results are based on specific attack types on actual locations that resulted in specific vulnerabilities. A vulnerability being a weakness in security measures which can be exploited by an

attacker to achieve their goal. As the actual outcome of these assessments are classified, the different vulnerabilities are also classified. However, upon analysis during the individual PRoTECT meetings (conducted in the five participating cities) and relevant European events which facilitated and triggered the exchange of information, knowledge and best practices on a cross-sectoral level, common needs were underlined regarding terrorism deterrence, prevention, situational awareness and timely emergency response. Furthermore, multiple needs have also been identified where technological solutions might be of support towards mitigating the vulnerabilities. These needs are categorized and are as follows:

- Enhancing the surveillance of an area to for instance count crowds, monitor allocation of citizens or identify occurrences of objects or behaviors. By enhancing this surveillance, a municipality and the other local actors can identify anomalies or assess the impact at certain moments in time before an attack or respond faster to incidents and aid citizens.
- Enhancing the cooperation between different actors (between own forces as well as completely different actors). In the cases of terrorist attacks, actors do not stand alone and need to cooperate in order to prevent, responds and recover from terrorist attacks. By enhancing the cooperation in could create more effective deployment of forces, better communication between them and faster (real time) sharing of information like images or videos to get ahead of the threat.
- Enhancing alerting and evacuating of citizens during an attack by putting in place early warning systems and effective evacuation pathways. Potential innovative technology solutions could enhance the warning systems and evacuation pathways for specific public spaces.
- Enhancing the existing knowledge and train forces specifically for protecting public spaces against terrorism, as anti-terrorism expertise is often missing at local government. There is a need of knowing were and how this knowledge can be obtained as well as how to train personal in the future.

These needs have been used to discuss the context for the technology exploration with the experts. A number of aspects of the technologies were considered for defining the technologies and indexing them in a useful way for the municipalities. The following paragraph describes the aspects in more detail.

9.3 Technology aspects

As mentioned above, the information gathered on technologies regards several aspects of the technologies, which are detailed in this section. These aspects can be used by a municipality to determine if the technology is useful for mitigating the vulnerability which the municipality is concerned about and what might need to be considered when choosing the technology.

Technology category. This aspect is beneficiary to scope the different technologies, identify relations between technologies and specific gaps of existing technologies. This aspect includes five categories that any technology should be linked to. The categories have been discussed and developed by all involved stakeholders. The five technology categories are:

1. *ICT* that could be used for communicating, storing, analysing and protecting information. Examples are: WiFi, IoT, Encryption, VPN, et cetera;
2. *Sensors* that could be used for detection, identification, localisation or tracking. Examples are: cameras, facial recognition, acoustic sniper localisation, et cetera;
3. *Actuators* that could be used for warning, intercepting or eliminating. Examples are: sirens, anti-drone drones, HPM vehicle stopping, et cetera;

4. *Physical measures* that could be used for controlling access, impeding an attack or protective materials. Examples are: tourniquets, portable rising steps, bomb blast window film, et cetera;
5. *Methods* that could be used for procedures, best practices or standards to implement solutions. An example is the ISO 31000 Risk Management.

Technology description. This aspect provides a short general description of the technology, include the name of the technology, the main technology principle and possibly some potentional strengths and weaknesses.

Threat types. This aspect concerns the type of threat a technology could be used against. The threat types are based on the EU VAT, because these are known to the five cities and have been used to identify vulnerabilities. The threat types are:

1. *Fire arms* attack - small calibre pistol or semi/full-automatic rifle;
2. *Sharp object* attack - knifes, machete, other sharp and blunt objects;
3. *Vehicle* attack - use of vehicle as a weapon by ramming large crowds;
4. *IED* (explosives) - left/concealed in objects or goods (based on home-made or commercial explosives);
5. *PBIED* (explosives) - explosives concealed on a person (suicide or carrier);
6. *UAVIED* (explosives) - explosives delivered by a remote-controlled airborne device;
7. *VBIED* (explosives) - explosives concealed inside a vehicle (or its cargo);
8. *Chemical* attack - threat object concealed in goods or carried items (e.g. canister or UAV dispensed);
9. *Biological* attack - threat object concealed in goods or carried items (e.g. canister or UAV dispensed);
10. *Radiological* attack - threat object concealed in goods or carried items (e.g. canister or UAV dispensed).

Threat phases. This aspect concerns the phase of an attack, for the attacker's perspective, for which the technology is applicable. The threat phases are:

1. *Initial Target Identification* (before the attack);
2. *Operational Planning* (before the attack);
3. *Pre-Attack Preparation* (before the attack);
4. *Execution* (during the attack);
5. *Post-Attack/Escape* (after the attack).

Technology use. Each technology is (part of) a security measure, providing some basic security function as a response to a (potential) threat. As used in the EU VAT, there are ten different technology uses that range from before, during and after an attack. The technology uses are:

1. *Alert* - used for alerting public (e.g. sirens, texting service);
2. *Surveil* - used for situational awareness (e.g. cameras, social media tools);
3. *Respond* - used for responding to an attack (e.g. security personnel, non-lethal weapons);

4. *Protect* - used to protect assets (people, buildings, infrastructure);
5. *Detect* - used for detecting a weapon or weapon use (e.g. entry scanning equipment);
6. *Overcome* - used for overcoming a sudden vulnerability (e.g. extra concertina wire);
7. *Improvise* - created on the spot from available means (e.g. use police vehicle as a road block);
8. *Restrict* - used for restricting public access (e.g. safety barriers);
9. *Adapt* - used for changing circumstances (e.g. moving assets to a safer location);
10. *Other.*

Technology common operational evaluation criteria. This aspect concerns criteria which are commonly used to evaluate a product using the technology or to compare products using the technology. For PRoTECT, only general criteria categories are mentioned. The criteria categories are:

1. *Physical* (weight, size, etc.);
2. *Cost* (purchase, hire, personnel, maintenance, etc.);
3. *Utilisation* (readiness, acquisition time, deployment time, interfacing, etc.);
4. *Compliancy* (privacy protection legislation, data protection directives, standards, etc.);
5. *Performance* (detection rate, failure rate, reaction time, intruder delay time, etc.);
6. *Other*.

Products/suppliers. It can be beneficiary to identify some existing products and/or suppliers, as examples, to have more understanding of the actual implementation of the technologies in commercially available products. This aspect could include the product names and types and/or the product manufacturer or suppliers.

9.4 Results

The explored technologies are categorized by the five technology categories and have been reported on the description, threat type, threat phase, technology use, technology criteria and potential products/suppliers. A full list of the explored technologies can be found in appendix IV. Here we mention a few overall results and how to use the overview of technologies.

As the SLR activity has focused on ICT solutions, this exploration of technologies has mostly focused on the other four technology categories. There are many technologies that can be categorized under sensor technology. These technologies range from specific weapon detectors to X-ray technologies to detection of deviant behavior by questioning to finally sensors to automatically start sprinkler systems. If looking further into these technologies, they are often usable for more than one type of threat, phase or use. The evaluation criteria stay generic and the most important criteria is 'performance'. This can articulate in detection rate or accuracy or failure rate. Both for actuator and physical technologies there are multiple technologies, that are also often linked to human behavior (for instance of the first responder or the surveillance team). Finally, the final category, method technologies, is standing out. However, the importance of resilience, training and decision making in protecting public spaces against terrorism is high and there are some technologies explored that can aid in these activities.

The technology overview can be used by municipalities to create more understanding of what is out there, how to look at technologies and create more awareness on the topic. Also, the table of technologies can be used by looking at the specific threat types, threat phases or technology use from the municipalities needs or gaps and find potentially relevant technologies. If relevant, this can be helpful in setting up the Request for Information or conducting the demonstration, in the next steps of the project. For a few of the technologies there is more information on example products (and sometimes a supplier). This gives the user some more insight in how a technology transforms into a product and how such a project could be used for a specific Public Space of Interest.

As a final note, the technology overview is not complete and is a living table that will be grow during the project. The upcoming project activities will gather and develop more insights in existing and future technologies that can be added to this overview of technologies.

10 Conclusions

Nowadays, the protection of public spaces is a big challenge that LEAs, municipalities and the European Commission are trying to tackle with the help of new available technologies.

The Deliverable 3.1 is intended to give a wide overview of technologies nowadays available both from scientific and market side. However, the aim of the deliverable is not only to give an analysis of the technologies available, instead to have a 360 degrees overview about what are the technologies, the architectural approaches and the prevention and management techniques to increase the level of privacy and security in our squares, our streets and more general in our cities.

From the systematic literature review the main finding is that there is no one single bullet solution available from the literature point of view. Conversely, it is important to use multiple methods and techniques to guarantee safety and security in public spaces. The techniques range from architectural design in order to rethink the design of public spaces keeping security into account in continuity to emerging technologies such as AI and predictive surveillance. Moreover, whenever new technologies could appear as not affordable from the municipalities due to the high costs, is always possible to build action plan in order to mitigate, prevent and manage crime events.

From the LEAs view viewpoint, the Deliverable 3.1 presents an overview on current solutions, novel solutions of tomorrow, and solutions in the far future for the protection of public spaces, which are implemented or tested in the security domain of local governments and LEAs.

From the European-Commission's viewpoint, the Deliverable 3.1 provided an overview of the ongoing projects that focus on the problem of the protection of public spaces we face today. The list has been provided in order to offer a starting point for future collaboration, improvements and enhancement of methods and techniques for the protection of public spaces.

Last, but not least, we provided an overview of technologies available for the protection of urban areas. In the 'ANNEX II. TECHNOLOGIES' we listed the technologies for mitigating vulnerabilities in the protection of public space. This has been done in order to build a first overview regarding the upcoming and available technologies, methods and approaches for the protection of public spaces.

In the light of PRoTECT, these activities aid the five beneficiary cities (but also any other local enforcement agency or municipality) to get more understanding of trends and available technologies out there, that can aid in mitigating vulnerabilities for protecting urban areas against terrorism.

References

Agarwal, S., & Sureka, A. (2015). Applying social media intelligence for predicting and identifying on-line radicalization and civil unrest oriented threats. *arXiv preprint arXiv:1511.06858*.

Agrawal, A., Fu, W., & Menzies, T. (2016). What is wrong with topic modeling?(and how to fix it using search-based se). *arXiv preprint arXiv:1608.08176*.

Allanach, J., Tu, H., Singh, S., Willett, P., & Pattipati, K. (2004). Detecting, tracking, and counteracting terrorist networks via hidden Markov models. *2004 IEEE Aerospace Conference Proceedings (IEEE Cat. No. 04TH8720)*, *5*, pp. 3246-3257.

Andersson, M., Gustafsson, F., St-Laurent, L., & Prevost, D. (2013, 2). Recognition of Anomalous Motion Patterns in Urban Surveillance. *IEEE Journal of Selected Topics in Signal Processing, 7*, 102-110. doi:10.1109/JSTSP.2013.2237882

Andreani, S., Kalchschmidt, M., Pinto, R., & Sayegh, A. (2019, 5). Reframing technologically enhanced urban scenarios: A design research model towards human centered smart cities. *Technological Forecasting and Social Change, 142*, 15-25. doi:10.1016/j.techfore.2018.09.028

Antiterrorismebeleid EU. (n.d.). Europa Nu. Retrieved from https://www.europa-nu.nl/id/vh1alt8tl1wf/antiterrorismebeleid_eu

Anuar, S., Selamat, A., & Sallehuddin, R. (2015, 1 1). Hybrid Artificial Neural Network with Artificial Bee Colony Algorithm for Crime Classification. *Computational Intelligence in Information Systems*. doi:10.1007/978-3-319-13153-5_4

Arunachalam, M., & Baboo, S. S. (2011). Enhanced Algorithms to Identify Change in Crime Patterns. *IJCOPI, 2*, 32-38.

Avidan, S. (2007, 2). Ensemble Tracking. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 29*, 261-271.

Bacchi, U., & Suliman, A. (2019). Face masks to decoy t-shirts: The rise of anti-surveillance fashion. Retrieved from https://www.reuters.com/article/us-britain-tech-fashion-feature/face-masks-to-decoy-t-shirts-the-rise-of-anti-surveillance-fashion-idUSKBN1WB0HT

Bonatsos, A., Middleton, L., Melas, P., & Sabeur, Z. (2013). Crime Open Data Aggregation and Management for the Design of Safer Spaces in Urban Environments. In *IFIP Advances in Information and Communication Technology* (pp. 311-320). Springer Berlin Heidelberg. doi:10.1007/978-3-642-41151-9_30

Borja-Borja, L. F., Saval-Calvo, M., & Azorin-Lopez, J. (2017). Machine Learning Methods from Group to Crowd Behaviour Analysis. In I. Rojas, G. Joya, & A. Catala (Ed.), *Advances in Computational Intelligence* (pp. 294-305). Cham: Springer International Publishing.

Boudihir, M. E., & Al-shalfan, K. A. (2012). INTELLIGENT VIDEO SURVEILLANCE SYSTEM ARCHITECTURE FOR ABNORMAL ACTIVITY DETECTION. *Keeping Pace with Criminals: Designing Patrol Allocation Against Adaptive Opportunistic Criminals.*

Boutry, T. (2019, 6). Suicide d'un rescapé du Bataclan : Guillaume, 131e victime du 13 novembre. Le Parisien. Retrieved from http://www.leparisien.fr/faits-divers/suicide-d-un-rescape-du-bataclan-guillaume-131e-victime-des-attentats-du-13-novembre-15-06-2019-8094099.php

Braun, V., Clarke, V., Hayfield, N., & Terry, G. (2018). Thematic analysis. *Handbook of research methods in health social sciences*, 1-18.

Brown, M., Saisubramanian, S., Varakantham, P., & Tambe, M. (2014). Streets: game-theoretic traffic patrolling with exploration and exploitation. *Twenty-Sixth IAAI Conference.*

Brussels explosions: What we know about airport and metro attacks. (2016, 4). BBC. Retrieved from https://www.bbc.com/news/world-europe-35869985

Buczak, A. L., & Gifford, C. M. (2010). Fuzzy association rule mining for community crime pattern discovery. *ACM SIGKDD Workshop on Intelligence and Security Informatics - ISI-KDD 10.* ACM Press. doi:10.1145/1938606.1938608

Calavia, L., Baladrón, C., Aguiar, J. M., Carro, B., & Sánchez-Esguevillas, A. (2012, 8). A Semantic Autonomous Video Surveillance System for Dense Camera Networks in Smart Cities. *Sensors, 12*, 10407-10429. doi:10.3390/s120810407

Camacho-Collados, M., & Liberatore, F. (2015, 7). A Decision Support System for predictive police patrolling. *Decision Support Systems, 75*, 25-37. doi:10.1016/j.dss.2015.04.012

Campedelli, G. M., Cruickshank, I., & Carley, K. M. (2018). Complex Networks for Terrorist Target Prediction. In *Social, Cultural, and Behavioral Modeling* (pp. 348-353). Springer International Publishing. doi:10.1007/978-3-319-93372-6_38

Chatfield, A. T., & Reddick, C. G. (2019, 4). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. *Government Information Quarterly, 36*, 346-357. doi:10.1016/j.giq.2018.09.007

Christmas attack: German government admits mistakes in aftermath. (2017, 12). BBC. Retrieved from https://www.bbc.com/news/world-europe-42410414

Chuang, J., Manning, C. D., & Heer, J. (2012). Termite. *Proceedings of the International Working Conference on Advanced Visual Interfaces - AVI 12.* ACM Press. doi:10.1145/2254556.2254572

Clutterbuck, R. L. (1990). *Terrorism and guerrilla warfare: Forecasts and remedies.* London: Routledge.

COMMISSION, E. U. (2017). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Action Plan to support the protection of public spaces. Retrieved from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_action_plan_to_improve_the_protection_of_public_spaces_en.pdf

COMMISSION, E. U. (2018). SECURITY UNION: PROTECTING PUBLIC SPACES EU MAYORS' CONFERENCE: ``BUILDING URBAN DEFENCES AGAINST TERRORISM''. Retrieved from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180308_security-union-protecting-public-spaces_en.pdf

Cong, Y., Gong, H., Zhu, S., & Tang, Y. (2009, 6). Flow mosaicking: Real-time pedestrian counting without scene-specific learning. *2009 IEEE Conference on Computer Vision and Pattern Recognition*, (pp. 1093-1100).

Crichton, D. (2018). We need to improve the accuracy of AI accuracy discussions. Retrieved from https://techcrunch.com/2018/03/11/accuracy-of-accuracy/

Cristani, M., Raghavendra, R., Bue, A. D., & Murino, V. (2013, 1). Human behavior analysis in video surveillance: A Social Signal Processing perspective. *Neurocomputing, 100*, 86-97. doi:10.1016/j.neucom.2011.12.038

Dalal, N., & Triggs, B. (2005). Histograms of Oriented Gradients for Human Detection. *Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05) - Volume 1 - Volume 01* (pp. 886-893). Washington: IEEE Computer Society. doi:10.1109/CVPR.2005.177

Dhiman, C., & Vishwakarma, D. K. (2019). A review of state-of-the-art techniques for abnormal human activity recognition. *Engineering Applications of Artificial Intelligence, 77*, 21-45.

Economist, T. (2019). Safe Cities Index 2019 - Urban security and resilience in an interconnected world. Retrieved from https://safecities.economist.com/wp-content/uploads/2019/08/Aug-5-ENG-NEC-Safe-Cities-2019-270x210-19-screen.pdf

EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT 2018 (TESAT 2018). (2018, 9). Retrieved from https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018

Feng, Y., Yuan, Y., & Lu, X. (2017). Learning deep event models for crowd anomaly detection. *Neurocomputing, 219*, 548-556.

Fricker, R. D., & Rolka, H. (2006, 9). Protecting against Biological Terrorism: Statistical Issues in Electronic Biosurveillance. *CHANCE, 19*, 4-14. doi:10.1080/09332480.2006.10722809

Garousi, G., Garousi, V., Moussavi, M., Ruhe, G., & Smith, B. (2013). Evaluating Usage and Quality of Technical Software Documentation: An Empirical Study. *Proceedings of the 17th International Conference on Evaluation and Assessment in Software Engineering* (pp. 24-35). New York, NY, USA: ACM. doi:10.1145/2460999.2461003

Garousi, V., Felderer, M., & Mäntylä, M. V. (2016). The need for multivocal literature reviews in software engineering: complementing systematic literature reviews with grey literature. In S. Beecham, B. Kitchenham, & S. G. MacDonell (Ed.), *EASE* (pp. 26:1-26:6). ACM.

Gigabyte. (2019). An Intelligent Video Analytics Platform. Retrieved from https://www.gigabyte.com/Solutions/AI-AIoT/intelligent-video

Grega, M., Matiolański, A., Guzik, P., & Leszczuk, M. (2016, 1). Automated Detection of Firearms and Knives in a CCTV Image. *Sensors, 16*, 47. doi:10.3390/s16010047

Guo, W. (201, 4 8). Common Statistical Patterns in Urban Terrorism. *under review, Apr 2019*.

Hache, V. (2016, 12). France arrests 11 people in Bastille Day truck attack in Nice. France 24. Retrieved from https://www.france24.com/en/20161212-french-police-arrest-11-suspects-over-nice-terrorist-attack

Hayajneh, A. M., Zaidi, S. A., McLernon, D. C., & Ghogho, M. (2016, 6). Drone Empowered Small Cellular Disaster Recovery Networks for Resilient Smart Cities. *Proc. Communication and Networking (SECON Workshops) 2016 IEEE Int. Conf. Sensing*, (pp. 1-6). doi:10.1109/SECONW.2016.7746806

Hendriks, T., & Laar, P. (2013). METIS: Dependable Cooperative Systems for Public Safety. *Procedia Computer Science, 16*, 542-551. doi:10.1016/j.procs.2013.01.057

Hikvision. (2017). Hikvision launches World's First ever 'Deep Learning' embedded NVR. Retrieved from https://www.hikvision.com/en/newsroom/latest-news/2017/hikvision-launches-world-s-first-ever--deep-learning--embedded-nvr/

Hsieh, H.-F., & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research, 15*, 1277-1288. doi:10.1177/1049732305276687

Huawei. (2019). X3221-C 2-Megapixel Super Starlight Facial Recognition IR Fixed Dome Camera. Retrieved from https://e.huawei.com/en/products/intelligent-video-surveillance/cameras/software-defined-camera/x3221-c

Jain, M., An, B., & Tambe, M. (2012, 8). Security Games Applied to Real-World: Research Contributions and Challenges. In *Moving Target Defense II* (pp. 15-39). Springer New York. doi:10.1007/978-1-4614-5416-8_2

Ji, S., Xu, W., Yang, M., & Yu, K. (2013, 1). 3D Convolutional Neural Networks for Human Action Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 35*, 221-231. doi:10.1109/tpami.2012.59

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational researcher, 33*, 14-26.

Kankanhalli, A., Charalabidis, Y., & Mellouli, S. (2019, 4). IoT and AI for Smart Government: A Research Agenda. *Government Information Quarterly, 36*, 304-309. doi:10.1016/j.giq.2019.02.003

Kavanaugh, A. L., Fox, E. A., Sheetz, S. D., Yang, S., Li, L. T., Shoemaker, D. J., . . . Xie, L. (2012, 10). Social media use by government: From the routine to the critical. *Government Information Quarterly, 29*, 480-491. doi:10.1016/j.giq.2012.06.002

Keyvanpour, M. R., Javideh, M., & Ebrahimi, M. R. (2011). Detecting and investigating crime by means of data mining: a general crime matching framework. *Procedia Computer Science, 3*, 872-880.

Khan, M. A., Welsh, D., & Roy, N. (2018, 3). Firearm Detection Using Wrist Worn Tri-Axis Accelerometer Signals. *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops).* IEEE. doi:10.1109/percomw.2018.8480345

Khan, Z. H., & Gu, I. Y. (2010, 9). Joint Feature Correspondences and Appearance Similarity for Robust Visual Object Tracking. *IEEE Transactions on Information Forensics and Security, 5*, 591-606.

Kiktova, E., Lojka, M., Pleva, M., Juhar, J., & Cizmar, A. (2015). Gun type recognition from gunshot audio recordings. *3rd International Workshop on Biometrics and Forensics (IWBF 2015)*, (pp. 1-6).

Kılıçlar, A., Uşaklı, A., & Tayfun, A. (2018, 6). Terrorism prevention in tourism destinations: Security forces vs. civil authority perspectives. *Journal of Destination Marketing & Management, 8*, 232-246. doi:10.1016/j.jdmm.2017.04.006

Kiryati, N., Raviv, T. R., Ivanchenko, Y., & Rochel, S. (2008, 12). Real-time abnormal motion detection in surveillance video. *Proc. 19th Int. Conf. Pattern Recognition*, (pp. 1-4). doi:10.1109/ICPR.2008.4761138

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering – A systematic literature review. *Information and Software Technology, 51*, 7-15. doi:https://doi.org/10.1016/j.infsof.2008.09.009

Ko, K.-E., & Sim, K.-B. (2018, 1). Deep convolutional framework for abnormal behavior detection in a smart surveillance system. *Engineering Applications of Artificial Intelligence, 67*, 226-234. doi:10.1016/j.engappai.2017.10.001

Kommenda, N., Holder, J., Clarke, S., Levett, C., Cage, F., Ulmanu, M., . . . Guest, P. (2017, 8). Barcelona van attack - a visual guide. Guardian News and Media. Retrieved from https://www.theguardian.com/world/2017/aug/17/what-happened-in-barcelona-las-ramblas-attack

Kouziokas, G. N. (2017). The application of artificial intelligence in public administration for forecasting high crime risk transportation areas in urban environment. *Transportation Research Procedia, 24*, 467-473. doi:10.1016/j.trpro.2017.05.083

Krippendorff, K. (1980). *Content Analysis: An Introduction to Methodology.* Beverly, Hills, CA: Sage Publications, Inc. Retrieved from http://www.amazon.ca/gp/product/0803914989/ref=wl_it_dp/702-0885532-1303250?ie=UTF8&coliid=I3UJ8HY4GH9OWF&colid=1DVGN4EKR6AVM

Kushwaha, A. K., Sharma, C. M., Khare, M., Srivastava, R. K., & Khare, A. (2012, 5). Automatic multiple human detection and tracking for visual surveillance system. *2012 International Conference on Informatics, Electronics & Vision (ICIEV).* IEEE. doi:10.1109/iciev.2012.6317384

Lega, M., Ferrara, C., Persechino, G., & Bishop, P. (2014, 8). Remote sensing in environmental police investigations: aerial platforms and an innovative application of thermography to detect several illegal activities. *Environmental Monitoring and Assessment, 186*, 8291-8301. doi:10.1007/s10661-014-4003-3

Li, S.-T., Kuo, S.-C., & Tsai, F.-C. (2010, 10). An intelligent decision-support model using FSOM and rule extraction for crime prevention. *Expert Systems with Applications, 37*, 7108-7119. doi:10.1016/j.eswa.2010.03.004

Life, T. N. (n.d.). Wide Area Motion Imagery (WAMI). Retrieved from https://www.tno.nl/en/focus-areas/defence-safety-security/roadmaps/information-sensor-systems/wide-area-motion-imagery-wami/

Liu, G., Liu, S., Muhammad, K., Sangaiah, A. K., & Doctor, F. (2018). Object Tracking in Vary Lighting Conditions for Fog Based Intelligent Surveillance of Public Spaces. *IEEE Access, 6*, 29283-29296. doi:10.1109/ACCESS.2018.2834916

Luo, X., Yuan, Y., Li, Z., Zhu, M., Xu, Y., Chang, L., . . . Ding, Z. (2019, 4). FBVA: A Flow-Based Visual Analytics Approach for Citywide Crowd Mobility. *IEEE Transactions on Computational Social Systems, 6*, 277-288. doi:10.1109/TCSS.2018.2877149

Mabrouk, A. B., & Zagrouba, E. (2018). Abnormal behavior recognition for intelligent video surveillance systems: A review. *Expert Systems with Applications, 91*, 480-491.

Magazine, D. S. (2017). Hikvision incorporates Deep Learning technology in its new line of cameras IP DeepinView. Retrieved from https://www.digitalsecuritymagazine.com/en/2017/11/02/hikvision-incorpora-la-tecnologia-deep-learning-nueva-linea-camaras-ip-deepinview/

Manchester Arena bomb: Service marks second anniversary. (2019, 5). BBC. Retrieved from https://www.bbc.com/news/uk-england-manchester-48369876

Matveev, A. V. (2016). Perspective Use of Modeling for Information Counter-Terrorism. *International Journal of Humanities and Cultural Studies (IJHCS) ISSN 2356-5926*, 2561-2567.

McCue, C. (2006). Data mining and predictive analytics in public safety and security. *IT Professional, 8*, 12-18.

Mehboob, F., Abbas, M., Rauf, A., Khan, S. A., & Jiang, R. (2019). Video Surveillance-Based Intelligent Traffic Management in Smart Cities. In *Intelligent Video Surveillance.* IntechOpen.

Melas, P., Correndo, G., Middleton, L., & Sabeur, Z. A. (2015). Advanced Data Analytics and Visualisation for the Management of Human Perception of Safety and Security in Urban Spaces. In *IFIP Advances in Information and Communication Technology* (pp. 445-454). Springer International Publishing. doi:10.1007/978-3-319-15994-2_45

Mills, E. (2017). 4 ways to design safer cities, and why we don't. Retrieved from https://www.marketplace.org/2017/08/25/4-ways-design-safer-cities-and-why-we-dont/

New England, U. (2019). *Grey literature*. Retrieved from https://www.une.edu.au/library/support/eskills-plus/research-skills/grey-literature

Nielsen, S. Z., Gade, R., Moeslund, T. B., & Skov-Petersen, H. (2014). Taking the Temperature of Pedestrian Movement in Public Spaces. *Transportation Research Procedia, 2*, 660-668. doi:10.1016/j.trpro.2014.09.071

Onan, A., Korukoglu, S., & Bulut, H. (2016). LDA-based Topic Modelling in Text Sentiment Classification: An Empirical Analysis. *Int. J. Comput. Linguistics Appl., 7*, 101-119. Retrieved from http://dblp.uni-trier.de/db/journals/ijcla/ijcla7.html#OnanKB16

Park, U., & Jain, A. K. (2010, 9). Face Matching and Retrieval Using Soft Biometrics. *IEEE Transactions on Information Forensics and Security, 5*, 406-415.

Popp, R., Armour, T., Numrych, K., & others. (2004). Countering terrorism through information technology. *Communications of the ACM, 47*, 36-43.

Radulov, N. (2019). ARTIFICIAL INTELLIGENCE AND SECURITY. SECURITY 4.0. *Security & Future, 3*, 3-5.

Rastyapina, O. A., & Korosteleva, N. V. (2016). Urban Safety Development Methods. *Procedia Engineering, 150*, 2042-2048. doi:https://doi.org/10.1016/j.proeng.2016.07.292

Recasens, A., Cardoso, C., Castro, J., & Nobili, G. G. (2013). Urban security in southern Europe. *European Journal of Criminology, 10*, 368-382. doi:10.1177/1477370812473535

Roberts, J. (2018). *Urban Safety Project Urban Safety and Security.* The Asia Foundation.

Rodionova, Z. (2016, 11). Bataclan survivor describes moment Isis gunman tried to kill her. Independent Digital News and Media. Retrieved from https://www.independent.co.uk/news/world/paris-attacks-one-year-anniversary-bataclan-survivor-kelly-le-guen-isis-islamic-state-a7413901.html

Rothkrantz, L. J. (2013). Crisis management using multiple camera surveillance systems. *ISCRAM.*

Sachan, A., & Roy, D. (2012, 4). TGPM: Terrorist Group Prediction Model for Counter Terrorism. *International Journal of Computer Applications, 44*, 49-52. doi:10.5120/6303-8516

Sarı, A., Tosun, A., & Alptekin, G. I. (2019). A systematic literature review on crowdsourcing in software engineering. *Journal of Systems and Software, 153*, 200-219.

Seidler, P., Haider, J., Kodagoda, N., Wong, B. L., Pohl, M., & Adderley, R. (2016). Design for intelligence analysis of complex systems: evolution of criminal networks. *2016 European Intelligence and Security Informatics Conference (EISIC)*, (pp. 140-143).

Shen, Q., Zeng, W., Ye, Y., Arisona, S. M., Schubiger, S., Burkhard, R., & Qu, H. (2018, 1). StreetVizor: Visual Exploration of Human-Scale Urban Forms Based on Street Views. *IEEE Transactions on Visualization and Computer Graphics, 24*, 1004-1013. doi:10.1109/TVCG.2017.2744159

Sievert, C., & Shirley, K. (2014). LDAvis: A method for visualizing and interpreting topics. *Proceedings of the Workshop on Interactive Language Learning, Visualization, and Interfaces.* Association for Computational Linguistics. doi:10.3115/v1/w14-3110

Singh, A., Patil, D., & Omkar, S. N. (2018). Eye in the Sky: Real-Time Drone Surveillance System (DSS) for Violent Individuals Identification Using ScatterNet Hybrid Deep Learning Network. *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 1710-17108.

Takizawa, A. (2011). Classification and feature extraction of criminal occurrence points using CAEP with transductive clustering. *Procedia - Social and Behavioral Sciences, 21*, 83-92. doi:10.1016/j.sbspro.2011.07.036

Tang, T., & Ho, A. T.-K. (2019, 4). A path-dependence perspective on the adoption of Internet of Things: Evidence from early adopters of smart and connected sensors in the United States. *Government Information Quarterly, 36*, 321-332. doi:10.1016/j.giq.2018.09.010

The cost of terrorism in Europe. (n.d.). Retrieved from https://www.rand.org/randeurope/research/projects/the-cost-of-terrorism-in-europe.html

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & security, 72*, 212-233.

Tseng, Y.-H., Ho, Z.-P., Yang, K.-S., & Chen, C.-C. (2012, 9). Mining term networks from text collections for crime investigation. *Expert Systems with Applications, 39*, 10082-10090. doi:10.1016/j.eswa.2012.02.052

Tutun, S., Khasawneh, M. T., & Zhuang, J. (2017, 7). New framework that uses patterns and relations to understand terrorist behaviors. *Expert Systems with Applications, 78*, 358-375. doi:10.1016/j.eswa.2017.02.029

Valasik, M. (2018, 9). Gang violence predictability: Using risk terrain modeling to study gang homicides and gang assaults in East Los Angeles. *Journal of Criminal Justice, 58*, 10-21. doi:10.1016/j.jcrimjus.2018.06.001

Verma, C., Malhotra, S., & Verma, V. (2018, 6). Predictive Modeling of Terrorist Attacks Using Machine Learning. *International Journal of Pure and Applied Mathematics, 119*.

Vincent, J. (2018). Artificial Intelligence Is Going To Supercharge Surveillance. Retrieved from https://www.theverge.com/2018/1/23/16907238/artificial-intelligence-surveillance-cameras-security

Vincent, J. (2018). Artificial Intelligence Is Going To Supercharge Surveillance. Retrieved from https://www.theverge.com/2018/1/23/16907238/artificial-intelligence-surveillance-cameras-security

Vincent, J. (2018). Drones taught to spot violent behavior in crowds using AI. Retrieved from https://www.theverge.com/2018/6/6/17433482/ai-automated-surveillance-drones-spot-violent-behavior-crowds

Wang, J., Ni, S., Shen, S., & Li, S. (2019, 6). Empirical study of crowd dynamic in public gathering places during a terrorist attack event. *Physica A: Statistical Mechanics and its Applications, 523*, 1-9. doi:10.1016/j.physa.2019.01.120

Wang, L. (2006). Abnormal Walking Gait Analysis Using Silhouette-Masked Flow Histograms. *Proceedings of the 18th International Conference on Pattern Recognition - Volume 03* (pp. 473-476). Washington: IEEE Computer Society. doi:10.1109/ICPR.2006.199

Wang, S., & Lee, H. (2007, 6). A Cascade Framework for a Real-Time Statistical Plate Recognition System. *IEEE Transactions on Information Forensics and Security, 2*, 267-282.

Wang, Z., Yin, Y., & An, B. (2016). Computing Optimal Monitoring Strategy for Detecting Terrorist Plots. *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence* (pp. 637-643). Phoenix: AAAI Press. Retrieved from http://dl.acm.org/citation.cfm?id=3015812.3015907

Welsh, D., & Roy, N. (2017, 3). Smartphone-based mobile gunshot detection. *Proc. IEEE Int. Conf. Pervasive Computing and Communications Workshops (PerCom Workshops)*, (pp. 244-249). doi:10.1109/PERCOMW.2017.7917566

Widyawan, Zul, M. I., & Nugroho, L. E. (2012, 11). Adaptive motion detection algorithm using frame differences and dynamic template matching method. *Proc. 9th Int. Conf. Ubiquitous Robots and Ambient Intelligence (URAI)*, (pp. 236-239). doi:10.1109/URAI.2012.6462984

Williams, T., & Betak, J. (2018). A Comparison of LSA and LDA for the Analysis of Railroad Accident Text. In E. M. Shakshuki, & A.-U.-H. Yasar (Ed.), *ANT/SEIT. 130*, pp. 98-102. Elsevier. Retrieved from http://dblp.uni-trier.de/db/conf/ant/ant2018.html#WilliamsB18

Woo, T. H. (2018, 8). Anti-nuclear terrorism modeling using a flying robot as drone's behaviors by global positioning system (GPS), detector, and camera. *Annals of Nuclear Energy, 118*, 392-399. doi:10.1016/j.anucene.2018.04.035

Wu, X., Dunne, R., Zhang, Q., & Shi, W. (2017). Edge computing enabled smart firefighting. *Proceedings of the fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies - HotWeb 17.* ACM Press. doi:10.1145/3132465.3132475

Zabłocki, M., Gościewska, K., Frejlichowski, D., & Hofman, R. (2014, 12). Intelligent video surveillance systems for public spaces – a survey. *Journal of Theoretical and Applied Computer Science, 8*, 13-27.

Zabłocki, M., Gościewska, K., Frejlichowski, D., & Hofman, R. (2014). Intelligent video surveillance systems for public spaces--a survey. *Journal of Theoretical and Applied Computer Science, 8*, 13-27.

Zhang, C., Sinha, A., & Tambe, M. (2015). Keeping Pace with Criminals: Designing Patrol Allocation Against Adaptive Opportunistic Criminals. *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems* (pp. 1351-1359). Richland: International Foundation for Autonomous Agents and Multiagent Systems. Retrieved from http://dl.acm.org/citation.cfm?id=2772879.2773326

Zhao, X., Wang, N., Han, R., Xie, B., Yu, Y., Li, M., & Ou, J. (2018, 3). Urban infrastructure safety system based on mobile crowdsensing. *International Journal of Disaster Risk Reduction, 27*, 427-438. doi:10.1016/j.ijdrr.2017.11.004

[1] PRoTECT Deliverable D2.1 "Manual for vulnerability assessment"

ANNEX I. BEST PRACTICES

FORENSOR - FOREnsic evidence gathering autonomous sensor GA 653355/H2020

The FORENSOR project aims to develop a novel, ultra-low-power, intelligent, miniaturised, low-cost, wireless, autonomous sensor ("FORENSOR") for evidence gathering. The combination of built-in intelligence with ultra-low power consumption will make this device a true breakthrough for combating crime. Covert evidence gathering has not seen major changes in decades. Law enforcement Agencies (LEAs) are still using conventional, manpower based techniques to gather forensic evidence. Concealed surveillance devices can provide irrefutable evidences, but current video surveillance systems are usually bulky and complicated, are often used as simple video recorders, and require complex, expensive infrastructure to supply power, bandwidth, storage and illumination.

Recent years have seen significant advances in the surveillance industry, but these were rarely targeted to forensic applications. The imaging community is fixated on cameras for mobile phones, where the figures of merit are resolution, image quality, and low profile. A mobile phone with its camera on would consume its battery in under two hours. Industrial surveillance cameras are even more power hungry, while intelligent algorithms such as face detection often require extremely high processing power, such as backend server farms, and are not available in conventional surveillance systems.

Coordinator: Bundesministerium Fuer Inneres;

BigClouT- Distributed Intelligence for Smarter Cities GA 723139/H2020

As the global population shifts towards urban areas, ICT solutions have the potential to change the way we live, work and play. Technologies like the internet of things (IoT), Big Data and cloud computing are particularly well-positioned as key enablers for increasing the efficiency of using shared urban infrastructures and natural resources.

Jointly funded by the EU and Japan, the BigClouT project is working to leverage these enabling technologies to give cities 'an analytical mind'. To do this, project researchers are developing distributed intelligence that can be seamlessly embedded within a city's network. "The project aims to provide cities with the analytic capability needed to exploit the Big Data coming from IoT devices, open data sources, social networks and mobile applications," explains project coordinator Levent Gürgen. "The goal is to improve the efficiency of cities and the lives of their citizens." From Big Data to smart applications.

The core of the project is an interoperable platform that accesses a vast set of heterogeneous data sources. Based on a modular architecture, the BigClouT platform is comprised of three levels. The first level collects and unifies data from a large variety of data sources (IoT devices, legacy platforms, web pages, mobile apps, etc.). The data is then redistributed to the second level, where it is processed for online and offline data analysis and visualisation. In the final layer, citizen-centric applications can be easily built with the provided service composition tools.

http://bigclout.eu

City Risk - Avoiding and mitigating safety risks in urban environments GA653747/H2020

City.Risks will leverage a set of innovative technologies, city infrastructures as well as Web and social media technologies aiming to increase the security level of citizens in large cities. Through City.Risks solution the citizens in modern smart cities will be actively contributing to the fight against crime and the increase of security level in their daily activities.

The project will rely on a wide spectrum of available technologies to design and implement an interactive framework among authorities and citizens through mobile applications that will allow in a collaboratively way to prevent or mitigate the impact of crime incidents or other security threats. Thus, it will contribute to an increase of the citizens' perception of security, which will be measured and validated in real-life scenarios and conditions through the deployment and operation of pilot trials at several selected cities by the project partners. Moreover, to further found its sustainability, the project will devise business models and replication plans of its results that will contribute in the next generation innovative security solutions for the future smart cities.

http://project.cityrisks.eu

SURVEIRON - Advanced surveillance system for the protection of urban soft targets and urban critical infrastructures GA 711264/H2020

SURVEIRON is an innovative solution for the protection of urban environments and critical infrastructures that provides those in charge of public and private security with an intelligent surveillance and decision making service in critical situations.

SURVEIRON constitutes a powerful tool for the prevention and management of potential disasters. Those in charge of coordinating security will be able to minimise the risks currently taken due to a scarcity of available information, which in general is provided solely by security cameras and telephone calls. Such gaps in the information available cause serious security problems.

The project is based in a set of AEORUMs intelligent robots embedded inside a fleet of unmanned aerial vehicles (UAVs). This fleet is deployed in fixed and mobile locations and supervised from an emergency command centre. When an alarm is notified, the system sends one or more UAVs to the emergency area avoiding any obstacle in their way. Once there, SURVEIRON starts scanning and analysing automatically the environment with different AEORUM detection technologies. All identified risks are sent to the control centre and represented in a 3D environment for an easy evaluation of human operators in real time. The system will also recommend action plans with AEORUM's decision making technologies based on artificial intelligence.

http://www.surveiron.com

SPIDERS - Synthetic aPerture Interferometric raDiometer for sEcurity in cRitical infraStructures GA 674274/H2020

Along with the evolution of nature and frequency of threats on various critical infrastructures and soft targets, there is a need for evolution and improvement in the detection solutions of hidden objects or materials that can represent a menace to European citizens and assets. Current long queues at airports or administration security checkpoints and bulky scanners will soon be seen as outdated with the coming technologies. As the number of transportation hubs and sensitive location for common security are increasing (airports, power plants, prisons, administrations) passive scanning system, not emitting any radiation, represent the most promising opportunities. Such systems require to tackle ethical issues such as the displaying of personal bodies and still be able to detect hidden objects. Other technical challenges have to be met in order to integrate such detection solution into the everyday life: 3D analysis, real-time detection, spatial resolution. SPIDERS project, built from the results of recent FP7 project to propose the latest passive millimetre wave technology with a synthetic aperture interferometric radiometer. The French company MC2, specialised in radiometric sensors and microwave products and services, aims at developing its business on the rising markets of PMMW technology for security applications and tackle all the stated technical and business challenges to demonstrate a fast 3D scanning system of walking people and detection of hidden objects and materials.

https://www.mc2-technologies.com

ChemSniff - Chemical sniffer device for multi-mode analysis of threat compounds GA 674716 H2020

ChemSniff will develop a multi-mode sniffer device for real-time detection of chemical compounds contained in CBRN-E substances. This will enable high throughput screening of soft targets such as vehicles, people and their personal effects.

The technology is based on a linear ion trap (LIT) mass spectrometer (MS) operating in a non-scanning mode. A non-scanning LIT allows selective ion monitoring of target threat molecules using optimal voltages for each ion mass without performing a full mass spectral scan. This result is higher sensitivity, simpler control electronics, smaller size, lower power consumption and cost. The limits of detection of LIT-MS instrument are in low parts per billion (ppb) with parts per trillion (ppt) levels achievable with suitable analyte enrichment provided by a pre-concentrator. Once the MS fingerprint of an unknown substance is measured, it can be compared online with a database of known substances enabling real-time rapid identification.

In 2014 pre-prototype instrument was demonstrated in FP7 Project SNIFFLES. ChemSniff will develop a more compact MS-based than existing instruments on the market with extra capability for rapid scans of solid surfaces using suitable atmospheric ionisation inlet. Methods for miniaturisation will be applied to all key components including the vacuum system, which is the most robust part. This will be done through improved designs based on results from numerical modelling, operational designs, novel low-cost 3D printing manufacturing, electronics simplification and vacuum system optimisation.

The final instrument will allow reduced acquisition/operating costs, greater mobility, user friendliness and flexibility. Performance will be benchmarked against a state-of-the-art conventional MS system for in-field analysis. The project outcome will be an automated portable MS-based sniffer device, tested and evaluated for a range of security applications and markets by end-users.

https://www.davinci-ls.com/en

BIO-AX - A novel wearable, cost-effective and non-invasive biometric body worn video solution for accurate and high throughput screening of people, bags and vehicles GA 719806/H2020

Body worn video systems are increasingly used to reduce threats and violence against police officers or other sensitive users like social workers, car parking inspectors, security guards, ambulance staff and firefighters. They can also be used as vital evidence in court. A novel system developed by Audax is taking the market to new heights.

The company envisions its BIO-AX camera as the future benchmark of the market. And it's not alone in doing so, if their award for the best communication system at the Counter Terror Awards 2018 is any indication. BIO-AX is the next-generation of complete Body Worn Video (BWV) camera ecosystem. It offers secure evidential video gathering together with active user protection and can transfer a live stream of video and audio footage (via 4G or Wi-Fi) to a command centre. The camera was designed to meet the New British Standard 8593:2017 on the deployment and use of BWV and is in full compliance with the New EU General Data Protection Regulation (GDPR). It packs high security, AES 256 encryption, GPS mapping and lone worker safety features into a rugged and lightweight product. It contains an enhanced staff 'safety blanket' alarm feature, with capability for remote access, remote memory wipe and even a 'man down' function.

BIO-AX connects directly to WiFi or 4G thanks to SIM card that freely chosen by the user. The camera also features text-to-speech (TTS) technology: users can type a message, send it to a camera or all cameras in a registered group, and the message is then played on the cameras' integrated speaker via Google Voice. Last but not least, BIO-AX it is designed and developed in the EU.

https://audaxsecurity.co.uk/bio-ax-all-in-one-camera/

INGENIOUS - The First Responder (FR) of the Future: a Next Generation Integrated Toolkit (NGIT) for Collaborative Response, increasing protection and augmenting operational capacity GA 833435/H2020

Today's First Responders (FR) are using technology of the past. During their primary mission of saving lives and preserving society's safety and security, FRs face a multitude of challenges. In both small scale emergencies and large scale disasters, they often deal with life-threatening situations, hazardous environments, uncharted surroundings and limited awareness. Threats and hazards evolve rapidly, crossing municipalities, regions and nations with speed and ease. Armouring public safety services with all the tools that modern technology has to offer is critical. Such tools holistically enhance their protection and augment their operational capacities, assisting them in saving lives as well as ensuring their safe return from the disaster scene.

INGENIOUS will develop, integrate, test, deploy and validate a Next Generation Integrated Toolkit (NGIT) for Collaborative Response, which ensures high level of Protection & Augmented Operational Capacity to respond to the disaster scene. This will comprise a multitude of the tools and services required:

1) for enabling protection of the FRs with respect to their health, safety and security;

2) for enhancing their operational capacities by offering them with means to conduct various response tasks and missions boosted with autonomy, automation, precise positioning, optimal utilisation of available resources and upgraded awareness and sense-making;

3) for allowing shared response across FR teams and disciplines by augmenting their field of view, information sharing and communications between teams and with victims. The NGIT armours the FRs at all fronts. The NGIT will be provided at the service of the FRs for extensive testing and validation in the framework of a rich Training, Testing and Validation Programme – of Lab Tests (LSTs), Small-Scale Field Tests (SSTs) and Full-Scale Field Validations (FSXs) – towards powering the FR of the future being fully aware, fully connected and fully integrated.

http://www.iccs.gr/

DRIVER+ DRiving InnoVation in crisis management for European Resilience GA 607798/ FP7-SECURITY

DRIVER+ starts from the experience that neither successful R&D nor strong end-user demand always lead to innovation in the Crisis Management (CM) domain. This is a problem since as societies become more complex, increasing scope and unpredictability of potential crises and faster dynamics of major incidents put increasingly stringent demands on CM. European CM capabilities already constitute a mature System of Systems; hence wholesale redesign would often be too costly and might critically destabilise existing CM capabilities. Therefore DRIVER+ focuses on augmenting rather than replacing existing capabilities. DRIVER+ has three main objectives: 1) Develop a pan-European Test-bed for crisis management capability development; 2) Develop a well-balanced comprehensive portfolio of crisis management solutions, and 3) Facilitate a shared understanding of crisis management across Europe.

The DRIVER+ Test-bed will provide the technological infrastructure, the necessary supporting methodology and adequate support tools. The Portfolio of Solutions (PoS) is a database driven web site that documents all the available DRIVER+ solutions. The PoS includes information on the experiences with a solution (i.e. results and outcomes of trials), the needs it addresses, the type of practitioner organisations that have used it, the regulatory conditions that apply, societal impact consideration, a glossary, and the design of the trials. Initially, the PoS will contain information about the solutions that are already available within the consortium; the PoS will be extended with third-party solutions when required by the trials, and ultimately opened up for any external organisation to share data and experiences on solutions.

A series of trials will be conducted during which solutions will be operationalised and tested. All results of the trials will be stored and made available in the PoS. Several I4CM events will be organized as well as a final conference. In addition to this, a firm link is established and will be maintained with DG HOME's "Community of Users on Secure, Safe and Resilient Societies" and other European stakeholder groups and relevant initiatives, for instance on standardization.

communication@projectdriver.eu

EXERTER Security of Exlosives pan-European Specialists Network GA 786805/H2020

EXERTER connects 22 practitioners from 13 EU Member States into a Network with Explosives Specialists within the Security of Explosives (SoE) area. The objective of the EXERTER Network is to bridge the difficulties for security practitioners to capture and utilize research results and to direct the industry's innovation efforts to address the most pressing needs in the fight against terrorism and serious crime. Practitioners will via EXERTER get improved operational capability via novel technologies, methods and knowledge to aid them in executing more efficient countermeasures in a changing threat environment. In cooperation with key practitioners in the Network, the project will each year define one unique scenario based on past events to facilitate the identification of capability gaps along different counter-terrorist phases associated with PREVENT, DETECT, MITIGATE and REACT. With its explosives expertise, EXERTER will provide recommendations to the SoE community on how these gaps can be countered by (i) directing innovators into targeted areas to which research programmes should focus, (ii) proposing standardization priority areas and (iii) advising on exploitation and commercialisation opportunities.

http://www.exerter-h2020.eu/

I-LEAD Innovation - Law Enforcement Agency's dialogue GA 740685/H2020

I-LEAD's focus is on the incapability of groups of operational Law Enforcement Agencies (LEA) practitioners defining their needs for innovation. This will be done in a methodological way, also with the help of the research & industrial partners supplemented by a broad range of committed stakeholders. I-LEAD will build the capacity to monitor the security research and technology market in order to ensure a better matching and uptake of innovations by law enforcement agencies with the overarching aim to make it a sustainable Pan-Europan LEA network. Earlier funded European research with a high technology readiness level as well as pipeline technologies will be closely monitored and assessed on its usefulness. Where possible a direct uptake from this research will be facilitated and implemented in the ENLETS and ENFSI networks supporting the action. I-LEAD will indicate priorities in five practitioner groups as well as aspects that needs (more) standardization and formulate recommendations how to incorporate these in procedures. As a final step, I-LEAD will advise the Member States through the existing EDBP-ESTP procurement group about how the outcomes of this project could be used in Pre-Commercial Procurement and Public Procurement of Innovation activities.

http://i-lead.eu/

ENTRAP Enhanced Neutralisation of explosive Threats Reaching Across the Plot GA 730560/ H2020

ENTRAP will deliver combined operational research (OR) methods for assessing and identifying emerging and future counter-measures. The tools will be used for identifying the needed step-changes for countering present, emerging and future explosive threats.

The OR tools will encompass methods including morphological analysis, attack-defence trees, Bow-tie diagrams and wargaming. The tools have been well-established for decades and they will be further developed and adapted for explosive threats. The proposed research aims to assess the effectiveness of counter-tools and their combinations across the plot. This will give a value on the efficiency they can provide

for historical cases or emerging and future scenarios for an attack. The project will strive to identify commonalities in the timeline where a counter-tool can be effective for several different scenarios. Thus, an effectiveness assessment will be made not only across the timeline for one scenario but also across different scenarios. The research and development efforts on a European level over the last decades will be a main source of background data. A gap analysis over the plot will in combination with the OR methods identify the need of required preventive counter-measures. A gap bridging assessment will together with the researcher and practitioner think-tank in ENTRAP ensure a step-change vision of counter-tools for important gaps. Historical attacks, scenarios defined in FP 7 projects, the EU Matrix group and NDE will be used as the basis. A cost assessment will be included giving an estimate for the required further developments. The ENTRAP consortium will bring together a world-leading team where the consortium includes 11 practitioners supported by an advisory board of key entities whereof 18 Letter of Supports have been obtained.

https://www.entrap-h2020.eu/en

IN-PREP - Crossing New Frontiers in Disaster Preparedness GA 740627/H2020

European countries confront the rising specter of transboundary crises, which cross national borders as well as policy boundaries with speed and ease, threatening the continuing functioning of critical infrastructures and the well-being of many citizens. Transboundary crises pose a specific set of complex challenges for which Europe is – despite recent policy initiatives (e.g. Decision No 1313/2013/EU) – still ill prepared. We recognize three challenges that need urgent attention.

First, member states need to develop shared response planning. Second, countries need to share information in real time. This sense-making challenge requires a way to have multiple countries and agencies create a shared picture of an emerging crisis based on multiple sources (different countries, many agencies). Third, countries need to coordinate the use of critical resources to ensure a timely response and to avoid waste and misspending. These challenges are hard to meet in any type of crisis or disaster, but especially in a transboundary context that lacks a dominant actor.

IN-PREP will establish and demonstrate a next generation programme by enabling a reference implementation of coordination operations (Handbook of Transboundary Preparedness and Response Operations that synthesises the lessons learnt, recommendations, check-lists from past incidents) and a training platform (Mixed Reality Preparedness Platform a novel IT-based tool, which holistically integrates Information Systems (IS) and Situational Awareness (SA) modules over a decision support mechanism and the visualisation of assets and personnel) to the entirety of civil protection stakeholders (firefighting units, medical emergency services, police forces, civil protection units, control command centres, assessment experts) to meet these challenges. The proposed framework will not only improve preparedness and planning but can be also applied during joint interventions, thus improving the joint capacity to respond.

https://www.in-prep.eu/

ASGARD - Analysis System for Gathered Raw Data GA700381/H2020

ASGARD has a singular goal, contribute to Law Enforcement Agencies Technological Autonomy and effective use of technology. Technologies will be transferred to end users under an open source scheme focusing on Forensics, Intelligence and Foresight (Intelligence led prevention and anticipation).

ASGARD will drive progress in the processing of seized data, availability of massive amounts of data and big data solutions in an ever more connected world. New areas of research will also be addressed. The consortium is configured with LEA end users and practitioners “pulling” from the Research and Development community who will “push” transfer of knowledge and innovation. A Community of LEA users is the end point of ASGARD with the technology as a focal point for cooperation (a restricted open source community). In addition to traditional Use Cases and trials, in keeping with open source concepts and continuous integration

approaches, ASGARD will use Hackathons to demonstrate its results. Vendor lock-in is addressed whilst also recognising their role and existing investment by LEAs. The project will follow a cyclical approach for early results. Data Set, Data Analytics (multimodal/ multimedia), Data Mining and Visual Analytics are included in the work plan. Technologies will be built under the maxim of "It works" over "It's the best". Rapid adoption/flexible deployment strategies are included. The project includes a licensing and IPR approach coherent with LEA realities and Ethical needs. ASGARD includes a comprehensive approach to Privacy, Ethics, Societal Impact respecting fundamental rights. ASGARD leverages existing trust relationship between LEAs and the research and development industry, and experiential knowledge in FCT research. ASGARD will allow its community of users leverage the benefits of agile methodologies, technology trends and open source approaches that are currently exploited by the general ICT sector and Organised Crime and Terrorist organisations.

http://asgard-project.eu/

CYBER-TRUST Advanced Cyber-Threat Intelligence, Detection and mitigation Platform for Trusted Internet of Things GA 786698/H2020

The CYBER-TRUST project aims to develop an innovative cyber-threat intelligence gathering, detection, and mitigation platform to tackle the grand challenges towards securing the ecosystem of IoT devices. The security problems arising from the flawed design of legacy hardware and embedded devices allows cyber-criminals to easily compromise them and launch large-scale attacks toward critical cyber-infrastructures. The proposed interdisciplinary approach will capture different phases of such emerging attacks, before and after known (even years old) or unknown (zero-day) vulnerabilities have been widely exploited by cyber-criminals to launch the attack. Emphasis is given on building a proactive cyber-threat intelligence gathering and sharing system to prevent the exploitation of zero-day vulnerabilities. This intelligence information will be used to maintain accurate vulnerability profiles of IoT devices, in accordance with data protection, privacy, or other regulations, and optimally alter their attack surface to minimise the damage from cyber-attacks. Novel technologies will be developed, based on distributed ledgers and blockchains, to monitor devices' integrity state and network behaviour that will considerably increase the detection and response capabilities against targeted and interdisciplinary cyber-attacks. In the case of alleged malicious activity, tools for collecting and storing forensic evidence on a tamper-proof blockchain structure will be delivered, taking into account the specific needs of law enforcement agencies. Privacy-preserving network monitoring and advanced virtual reality-based visualisation techniques will be employed for quickly detecting botnets, DDoS attacks and other incidents. Relying on interdisciplinary research, an intelligent autonomous cyber-defence framework will be built for providing intelligent ways of isolating the devices under an attacker's control (or infected) and effectively responding to and mitigating large-scale attacks.

ASTRID Adressing ThReats for virtualized services GA 786922/H2020

The growing adoption of cloud technologies and the trend to virtualise applications are inexorably re-shaping the traditional security paradigms, due to the increasing usage of infrastructures outside of the enterprise perimeter and shared with other users. The need for more agility in software development and maintenance has also fostered the transition to micro-services architectures, and the wide adoption of this paradigm has led service developers to protect their applications by including virtualised instances of security appliances in their design. Unfortunately, this often results in security being managed by people without enough skills or specific expertise, it may not be able to cope with threats coming from the virtualization layer itself (e.g., hypervisor bugs), and also exposes security appliances to the same threats as the other application components. It also complicates legal interception and investigation when some applications or services are suspected of illegal activity.

To overcome the above limitations, the ASTRID project aims at shifting the detection and analysis logic outside of the service graph, by leveraging descriptive context models and their usage in ever smarter

orchestration logic, hence shifting the responsibility for security, privacy, and trustworthiness from developers or end users to service providers. This approach brings new opportunities for situational awareness in the growing domain of virtualised services: unified access and encryption management, correlation of events and information among different services/applications, support for legal interception and forensics investigation.

ASTRID will develop a common approach easily portable to different virtualisation scenarios. In this respect, the technology developed by the Project will be validated in two relevant domains, i.e., plain cloud applications and Network Function Virtualisation, which typically exploits rather different chaining and orchestration models.

https://www.astrid-project.eu/

TENSOR Retrieval and analysis of heterogenous online content for terrorist activity recognition GA 700024/H2020

Law Enforcement Agencies (LEAs) across Europe face today important challenges in how they identify, gather and interpret terrorist generated content online. The Dark Web presents additional challenges due to its inaccessibility and the fact that undetected material can contribute to the advancement of terrorist violence and radicalisation. LEAs also face the challenge of extracting and summarising meaningful and relevant content hidden in huge amounts of online data to inform their resource deployment and investigations.

In this context, the main objective of the TENSOR project is to provide a powerful terrorism intelligence platform offering LEAs fast and reliable planning and prevention functionalities for the early detection of terrorist organised activities, radicalisation and recruitment. The platform integrates a set of automated and semi-automated tools for efficient and effective searching, crawling, monitoring and gathering online terrorist-generated content from the Surface and the Dark Web; Internet penetration through intelligent dialogue-empowered bots; Information extraction from multimedia (e.g., video, images, audio) and multilingual content; Content categorisation, filtering and analysis; Real-time relevant content summarisation and visualisation; Creation of automated audit trails; Privacy-by-design and data protection.

The project brings together industry, LEAs, legal experts and research institutions. It is expected that this collaboration will have significant impact on 1) ensuring the final system meets end-user LEA requirements, 2) enabling LEAs to access and examine terrorist generated content online bringing significant advantages to their operational capability, and 3) promoting industry's enhanced understanding of operational LEA requirements and their market competitiveness in the field of online organised crime, terrorism and harmful-radicalisation.

https://tensor-project.eu/

PROPHETS - Preventing Radicalisation Online through the Proliferation of Harmonised ToolkitS GA 786894/H2020

PROPHETS will look at redefining new methods to prevent, investigate and mitigate cybercriminal behaviours through the development of a coherent, EU-wide, adaptive SECURITY MODEL, built upon the interplay of the human factors within the new cyber ecosystem and capable of addressing the four fundamental dimensions at the core of the phenomenon: 1. early identification of security threats; 2. investigations within a new public-private governance; 3. Increased complexity of the response due to the expansion of the security perimeter towards new societal fields and the emergence of challenging jurisdictional problems; and, last but not least, 4. perception of security and freedoms among citizens, which requires a new communication strategy for LEAs and security policy makers.

Coordinated by: HOCHSCHULE FUR DEN OFFENTLICHEN DIENST IN BAYERN Germany

EVAGUIDE - Security management Platform for enhanced situation awareness and real-time adaptive evacuation strategies for large venues for sports and entertainment GA831154/H2020

evaGuide is a Security Management Platform for enhanced situation awareness and real-time adaptive evacuation strategies for large venues for sports and entertainment. evaGuide aims to address the needs of the safety of large facility visitors during complex evacuation processes, following normal and abnormal events (crises) towards the creation of an easily deployable system that will be able to timely identify new threats, designate and sustain a Location based Dynamic Evacuation Route (LDER) that improves all corresponding response times under any circumstances. Moreover it will support the complete lifecycle of evacuation planning, simulating complex scenarios, training of safety personnel and assessment of the performed actions. The results of the market research that has been performed among the 300 member stadia of ESSMA (the European Stadium & Safety Management Association) revealed that there is a clear need for a project like evaGuide that addresses all the phases of the evacuation lifecycle and offers superior situational awareness, while at the same time existing and emerging regulations from FIFA/UEFA need to be met. The business sustainability/exploitation potential has been validated in the Feasibility Study, which is an integral part of this proposal. The project outcome will be a fully functional evaGuide platform demonstrator delivered for operational use to one stadium (one of the ESSMA member stadia, selected on M2). The demonstrator will perform according to the adapted requirements defined by ESSMA and the stakeholders involved (finalized on M10), will be fully integrated (by M20) and tested (M21), ready to be commercially exploited by the joint commercialization entity defined during the last months of the project (M24).

http://www.telesto.gr/

BULLSEYE harmonize the different existing procedures and the used equipment in the EU countries to respond to a chemical or a biological terrorist attack GA 815220 ISFP-2017-AG-PROTECT

The aim of Bullseye is to harmonize the different existing procedures and the used equipment in the EU countries to respond to a chemical or a biological terrorist attack. First step is a gap analysis concerning the existing procedure and equipment. Next step is will be the organization expert meetings where first responders (police, medics, fire fighters, civil protection, military, DVI, forensics, labs) of the 5 involved countries in the project exchange knowledge and procedures based on the gap analysis and discuss them with C and B experts to get a harmonized draft. These procedures and equipment will be tested and trained per group of first responders and will be finally evaluated in a cross-sectoral exercise. Taken the lessons-learnt into account of these trainings and exercise, the procedures and tools will be fine-tunes, adapted and validated. Finally, a train the trainer course is developed that can be used for all first responders of the EU.

Coordinator: Service Public Federal Interieur

Pericles - Preventing vehicle ramming attacks GA 815358 ISFP-2017-AG-PROTECT

Vehicle-ramming attacks against human targets constitute a relative new threat. The general objective of the PERICLES project is to better prevent and respond to vehicle-ramming attacks by improving physical security measures in public spaces as well as the skills of law enforcement on how to respond to vehicle ramming attacks. The project will also raise the awareness of the public on how to react in case of such an attack. The project will develop a comprehensive European vulnerability tool that will allow authorities to assess their public spaces. There will be a focus on security by design in which aesthetics and the open nature of public spaces are taken into account in order to minimize the impact on society. The project aims also at improving skills of EU LEA's on how to respond to vehicle ramming attacks. Lastly, a public awareness campaign for the members of the general public will be created.

Coordinator: Politiezone Van Antwerpen

PACTESUR Protect Allied Cities against TErrorism in Securing Urban aReas GA 815091 ISFP-2017-AG-PROTECT

Protect Allied Cities against TErrorism in Securing Urban aReas. The objective is to improve cities capacity to secure their urban areas against terrorism.

PACTESUR's consortium involves three flagship cities (Nice, Torino, Liège) committed to strengthening their cooperation and having convergent strategies on urban security and three partners (ANCI, EFUS, NCA). 10 more cities will be selected and engaged as associated cities by February 2019.

Events will be organized in the three partner cities during the "European week of security": Nice in October 2019, Torino in 2020 and Liège in 2021. This will include a 3 day training dedicated to police forces. European experts will deal with how the legal frames could evolve as regards of the organization of police forces resulting in an in-depth study and recommendations.

The main project outcome is a well-structured framework defining how cities and local police forces can better protect their vulnerable public spaces.

Coordinator: Commune De Nice;

MELODY "A harmonised CBRN training curriculum for first responders and medical staff" GA 814803 ISFP-2017-AG-PROTECT

The main objective of the project is to define, develop and deploy a harmonized CBRN training curriculum for first responders and medical staff. The idea is to combine existing training curricula to develop a course which will suit first responders of Europe as good as possible. The improved CBRN training curriculum will be assessed and evaluated through a number of dedicated exercises and training activities with practitioners from different countries, which will lead to further improvements.
The resulting course will be demonstrated and disseminated to showcase it through a set of full scale exercises, and to raise awareness of it at all levels: from practitioners to policy makers.
The fully fit-for-purpose CBRN training curriculum for EU first responders and medical staff, properly quality assured and controlled will be delivered three years after the initiation of the project.
Coordinator: Studiecentrum Voor Kernenergie

XClanLab Application for mobile devices to identify a clandestine laboratory for homemade explosives GA 815359 ISFP-2017-AG-PROTECT

Members of the uniformed police or the rescue services seldom have experience and knowledge on homemade explosives. For their own safety, for being able to take control of the situation and to preserve possibilities for criminal investigations that will follow, it is of utmost importance that these authorities are able to recognize a bomb factory from the items they see on the site. It is important that they know how to act in such a situation and how to be safe as well as what information to convey to experts. This project will develop a mobile application (app) for Android and IOS operated devices to meet these requirements. The contents will include photos of typical chemicals and equipment. There is also a report function included where information as well as photos from the scene can be transferred to experts.

Coordinator: Bundeskriminalamt

SECUR-CITIES Prévention et sécurité dans les espaces publics des villes européennes GA 815391 ISFP-2017-AG-PROTECT

Recent terrorist attacks across Europe have highlighted the need for new security equipment to better protect potential targets, the need to rethink urban planning and to develop a genuine safety culture. The

Secur'Cities project, implemented by the cities of Lyon and Barcelona, aims to strengthen the protection measures in the public area by all actors. The objective of the project is twofold:

1. Develop new local approaches to secure public spaces and develop exchanges of practices on this matter;
2. Test new equipment and technologies to improve public safety.

These two components will allow to:

. Preserve the free nature of public spaces while ensuring that the population retains its quality of life;
. Curb and minimize the impact of possible new attacks.
. Improve the mobilizations of the various security and relief services.
. Put in place a transferable model for other European cities.

Coordinator: Commune De Lyon

PRINCE Preparedness Response for CBRNE incidents GA 815362 ISFP-2017-AG-PROTECT

The project PRINCE aims to support first aid responders and law enforcement authorities by providing them with an evidence base for strategic level decisions related to Prevention, Detection, Respiratory Protection, Decontamination and Response to CBRNE events. PRINCE aims to:
Produce a roadmap and recommendations by creating a PRINCE catalogue of training curricula based on best practices and international proven CBRNE exercises and produce CBRNE SOPs and plans for 2 incidents (Chemical and Radiological) in two major exercises (GR, PT) and includes sharing information on CBRN threat and risks, exchange best practices and joint trainings and exercises.
Enhance protection of public spaces, community and infrastructure by sharing project outcomes with wider audience through online information material, presentations to public events and media and increases the sustainability by exchanging best practices and knowledge on joint exercises and training courses between stakeholders.
Coordinator: Ypiresia Diacheirisis Europaikon Kai Anaptyxiakon Programmaton (Y.d.e.a.p.)

SafeCi - Safer Space for Safer Cities GA 814892 ISFP-2017-AG-PROTECT

The two-year project "Safer Space for Safer Cities" ("SafeCi") aims at enhancing the protection of public spaces and other soft targets in the light of the omnipresent terrorist threat. The European dimension is guaranteed as police forces from DE, BE, LU, ES, PT, CZ, SE, IE, AT, FI are project partners. The following topics will be tackled:

- Permanent and mobile barrier systems
- Traffic route security
- Protection of critical infrastructures
- Risk assessment for public spaces
- Awareness strategies
- Dealing with drones

In joint workshops the focus topics will be developed. Peer reviews will identify good practice and lessons learnt by the partners and finally a handbook with recommendations will be presented. In the end a network of actors in the field shall be formed. Cooperation between special police units, with regional and local authorities and beyond European borders shall be improved. Cross-sector expertise shall compliment all work packages.
Coordinator: Der Polizeiprasident In Berlin

SHERPA - Shared and coherent European Railway Protection Approach GA 815347/ISFP-2017-AG-PROTECT

The SHERPA project aims at improving the overall protection level for stations and trains in Europe against terrorist attacks by implementing multiple synergistic actions towards the relevant stakeholders, such as: providing and sharing an up-to-date, high-value knowledge base on threats and countermeasures (both technical and procedural); defining a coherent approach for risk assessment, risk management, crisis and disaster recovery management; strengthening co-operation among stakeholders through high-level international trainings and other practical tools; outlining needs and requirements for industry and research to focus on to better help railways in coping with both present and future threats.

The project is led by UIC Security division. Five among the most relevant key-players in the European railway sector (DB, FS, PKP, SNCB, SNCF) take part as co-applicants in SHERPA.

Coordinator: Union Internationale Des Chemins De Fer;

Skyfall - LEA training for Counter-UAV Protecting europe against UAV threats GA 815244/ISFP-2017-AG-PROTECT

The number of drones in use (by consumers) will exponentially grow in the next coming years. As the number of drones increases, the number of misuse will be expected to do too. A major concern is the threat that terrorists can use (weaponised) UAVs to carry-out attacks. As the chances of misuse of UAV's increases, European Law Enforcement Agencies should improve their preparedness and response levels in order to properly counter this threat and safeguard the security of the European citizens.

Skyfall will develop a European matrix how to protect and respond on different types of UAV incidents, in relation to the location and the kind of event that is going on. Secondly, the project will make a study of all systems currently available, which are suitable for physical drone interception.

Coordinator: Politiezone Van Antwerpen, Romanian Gendarmerie

31 CERBERUS - The establishment of the Central European Regional Mobile CBRN-E/Dirty Bomb First Responder Unit GA 815310/ISFP-2017-AG-PROTECT

The CERBERUS project aims to establish the Central European Regional Mobile CBRN-E/Dirty Bomb First Responder Unit. This initiative will create and maintain a regional, mobile, first responder capability to address the threats posed by the illicit use of chemical, biological, radioactive and nuclear (CBRN) materials especially when they are combined with explosives devices (hereinafter: dirty bomb). Project CERBERUS will create a response capability and develop a unique cross border and cross-sectoral cooperation and coordination mechanism for CBRN-E/dirty bomb first responders that currently does not exist within the European Union. The project also focuses on the professional CBRN-E knowledge maintenance as well, that includes the improvement of the training facilities of the Centre.

Coordinator: Keszenleti Rendorseg

DirtyBomb- Increased preparedness to CBRN incidents via first responders' joint exercises GA 815151/ISFP-2017-AG-PROTECT

The project`s aim is to enhance the level of preparedness of first responders to CBRN incidents through verification of a current readiness of services to react to terrorist attacks with the use of the so-called "dirty bomb", identification of critical points to be improved and development of training materials for the EU LEAs. The project foresees gathering information on schemes of conduct in the partners` countries to a "dirty bomb" threat and then - to conduct scenario-based activities for services, including realization police unit officer (RPUOs) from EU countries, in order to check the current state of preparation and practical knowledge of participants.

Then, a training session will be held to discuss the mistakes and correct procedures. After that a second exercise will be held, this time focusing on using the recommended procedures. Both days of exercises will be summed up with a detailed discussion and consolidation of the right patterns of conduct.
Coordinator: Komenda Stoleczna Policji

ATLAS 2017- a transnational network of 38 special intervention units from all 28 EU-MS and Iceland, Norway and Switzerland organizing joint trainings and exercises in maritime and urban environment GA814730/ISFP-2017-AG-IBAATLAS

ATLAS is a transnational network of 38 special intervention units from all 28 EUMS and Iceland, Norway and Switzerland. On the basis of the Council Decision 2008/617/JHA of 23 June 2008, ATLAS is organizing joint trainings and exercises in maritime and urban environment. Thereby, tactical and technical intervention skills are improved and standardized. Different theme-groups deal with the current challenges: Counter-Terrorism, aircraft-hijacking, naval based operations, basic life support in hostile environments and "Rapid Response" tactics. Furthermore, the use and the improvement of special technics, e.g. "drones", is continuously explored.

Coordinator: Bundesministerium Fuer Inneres;

ENLETS ETP - GA 814756 /ISFP-2017-AG-IBAENLETS

ENLETS is an active network of Law Enforcement agencies that are sharing best practices, activates co-creation and stimulates research for law enforcement. The activities of ENLETS are supported by the European Commission and the European Agencies, such as Europol, Eu-Lisa and EU-Lisa.
ENLETS was created under the auspices of the Law Enforcement Working Party. From 2008 until 2012 participation in the ENLETS network was promising, though the group was in search for concrete plans and actions. In 2012 new vigour was brought into the group by refreshing the vision and mission of ENLETS. A representation of Member States was formed into a Core Group with a Core Group Leader to enhance daily activities.
The National Police Of The Netherlands

RAILPOL - GA 821848/ISFP-2017-AG-IBARAILPOL

RAILPOL is an international association of governmental controlled police organisations responsible for policing the railways in Europe. The aims are to enhance and intensify international railway police cooperation, to prevent threats, to guarantee the effectiveness of measures against cross-border crime and to be the link between the police and the railway sector. RAILPOL have several working groups handling specific topics, thus improving the exchange of (operational) information and techniques. RAILPOL promotes public private partnership and strives for cooperation with stake holders and International law enforcement organisations.

The strength of RAILPOL lies in the direct contact with the organisations within RAILPOL responsible for railway policing. RAILPOL is a unique and solid platform for cross-border law enforcement cooperation in the railway environment. With active members and support from the European Commission, RAILPOL strives further to make Europe more secure.

The National Police Of The Netherlands

STEPWISE - A Simulation, Training, and Evaluation Platform for the Protection of Crowded Public Spaces GA 815182/ISFP-2017-AG-PROTECT

The STEPWISE project arises in the context of the terrorist attacks perpetrated in Europe and the EU plan released in October 2017 on the protection of public spaces. The aim was to help member states better protect their public spaces, reduce vulnerabilities and prevent future attacks, particularly on sensitive sites.
STEPWISE will support: the creation of digital models of places and buildings, the study of security design, assessing the degree of vulnerability of public spaces, sharing of knowledge on the protection of public spaces.
The ultimate goal is, on the one hand, to be able to make prototypes of sensitive sites on models of visual realities and to list threat scenarios, and on the other hand, to reinforce the collaboration between the actors in charge of the protection of public spaces.
Diginext

beAWARE - Integrated solution to support forecasting, early warnings, transmission and routing of emergency data, aggregated analysis of multimodal data, and management tha coordination between the first responders and the authorities GA 700475/H2020

In every disaster and crisis, incident time is the enemy, and getting accurate information about the scope, extent, and impact of the disaster is critical to creating and orchestrating an effective disaster response and recovery effort. The main goal of beAWARE is to provide support in all the phases of an emergency incident. More specifically, we propose an integrated solution to support forecasting, early warnings, transmission and routing of the emergency data, aggregated analysis of multimodal data and management the coordination between the first responders and the authorities. Our intention is to rely on platforms, theories and methodologies that are already used for disaster forecasting and management and add the elements that are necessary to make them working efficiently and in harm under the same objective. The overall context for beAWARE lies in the domain of situational awareness and command and control (C2). The first phase concerns the forecast of the extreme condition and the relevant preparations. Once a disaster occurs, an initial assessment needs to be conducted as soon as possible to determine the scope, geographical distribution, and scale of the incident. Situational awareness means being able to accurately determine what has happened, what is happening now, and what will come next, all in order to plan and coordinate the most effective response possible with the resources available. This observation phase will lead to an orientation phase suggesting both an individual as well as collective “cognition” orientation to data that is sensed and communicated. Once orientation to the data (or the lack of it) occurs then a decision is made, ultimately resulting is the final step, which is “act”. The crisis management centre is always striving or struggling to gain a sense of what is reality to be able to feel that he or she can make a decision that is the "best possible" given the circumstances.

https://beaware-project.eu/

MAGNETO - Multimedia Analysis and correlation enGine for orgaNised crimE prevenTion and investigation GA 786629/H2020

MAGNETO addresses significant needs of law enforcement agencies (LEAs) in their fight against terrorism and organised crime, related to the massive volumes, heterogeneity and fragmentation of the data that officers have to analyse for the prevention, investigation and prosecution of criminal offences. These needs have been identified after consulting with eleven different European LEAs –members of the MAGNETO consortium. In response, MAGNETO empowers LEAs with superior crime analysis, prevention and investigation capabilities, by researching and providing tailored solutions and tools based on sophisticated knowledge representation, advanced semantic reasoning and augmented intelligence, well integrated in a common, modular platform with open interfaces. By using the MAGNETO platform, LEAs will have unparalleled abilities to fuse and analyse multiple massive heterogeneous data sources, uncover hidden relationships among data items, compute trends for the evolution of security incidents, ultimately (and at a faster pace) reaching solid evidence that can be used in Court, gaining also better awareness and

understanding of current or past security-related situations. In parallel, MAGNETO will spark an ecosystem of third-party solution providers benefiting from its open, modular and reusable architectural framework and standard interfaces.
To achieve these objectives, MAGNETO will test and demonstrate its developments on five representative and complementary use cases (types of crime), under real-life operational conditions in the facilities of eleven different LEAs, keeping them continuously in the production loop, adopting an agile implementation methodology and a multi-disciplinary scientific approach, combining researchers with exceptional track records, officers with top-level operational know-how in law enforcement, recognised experts for legal and ethical compliance to EU and national standards, and qualified training experts for innovative curricula development.
http://www.magneto-h2020.eu/

MEDEA - Mediterranean practitioners' network capacity building for effective response to emerging security challenges GA 787111/H2020

The "Mediterranean practitioners' network capacity building for effective response to emerging security challenges – MEDEA" is an EU funded (Cf. Grant Agreement 787111) Coordination and Support Action (CSA) in the topic of SEC-21-GM-2016-2017. The MEDEA's scope is to establish and further develop a regional Networks of practitioners and other security related actors in the Mediterranean and the Black Sea region.
The MEDEA practitioners are from different disciplines and they represent a variety of interests and expectations from Research, Development and Innovation (RDI) initiatives. To avoid a diversified register of fragmented operational needs, the consortium will process a regional exposure to risks and threats using the following four Thematic Communities of Practitioners (TCP): Managing of migration flows and asylum seekers, Border management and surveillance, Fight against cross border organized crime and terrorism, Natural hazards and technological accidents.
https://www.medea-project.eu/

CITYCOP - Citizen Interaction Technologies Yield Community Policing GA 653811/H2020

CITYCoP aims to develop an application which will facilitate, strengthen and accelerate the communication between citizens and police forces, by making it possible for community representatives to identify the risk and immediately report it.
The design of the detailed functionality specifications for the CITYCoP system will consist of four tools:

- a portal,
- a central back-end system,
- a mobile app
- a social media infrastructure.

The system should be capable of incorporating most of the functionalities identified in the previous phases of the project. Furthermore, the detailed specifications will also include specifications on integration of the different aspects of the CITYCoP system application.
Five pilot cities (BUCHAREST, LISBON, FLORENCE AND DUBLIN AND KILDARE) have been selected to test the CITYCoP system developed by the project, where a training scheme will be developed to assist both officers and citizens in the uptake of the solution.
Tools or toolkits resulting from such projects
1. Privacy-by-design methodology .
2.Training game for LEA officers based on scenario building and reaction.
http://www.citycop.eu/the-citycop-project/the-portal-and-app/the-portal-and-app.kl

TRILLION TRusted, CItizen - LEA coILaboratIon over sOcial Networks GA 653256/H2020

The TRILLION project aims to improve the collaboration between citizens and LEAs by providing multiple channels for incident reporting and interaction, fostering trust among parties and involving the discovery, acquisition, extraction and inferential analysis of relevant information from public sources according to privacy and regulations at EU and national levels. TRILLION will also increase situational awareness by supporting LEAs in decisional processes of intervention, in order to ensure full alignment to the needs of citizens.
The project will improve prevention of critical situations before they escalate by easing real-time information about identified risks from citizens to police forces. This goal is reached by facilitating information sharing and effective collaboration between citizens and LEAs
Community building is not just the creation of a relationship between LEAs and citizens, but it should be based on trust and cooperation strenghening the community feeling and lower feeling of insecurity. Cooperation and collaboration will ensure security and privacy.

http://trillion-project.eng.it/#/progetto-trillion

VALCRI - Visual Analytics for Sense-making in CRiminal Intelligence analysis GA 608142/FP7-SECURITY

Big data, its dizzying volumes of information flowing from multiple sources and the lack of perspective on these sources means it's really difficult to make sense of information in moments of urgency. As Andrew Parker, Director of the MI5 once explained, 'we only ever have fragments of information, and we have to try to assemble a picture of what might happen, based on those fragments.' This problem started coming to light with the 9/11 terrorist attacks, and has been plaguing investigations up until the most recent attacks. However, a solution is now presenting itself.

The VALCRI (Visual Analytics for Sense-making in CRiminal Intelligence analysis) project consortium is in the final development stages of a criminal intelligence analysis system based on visual analytics and cognitive engineering.

The system uses dedicated engines to identify similarities, performs associative searching and comes up with reports in the same area and timeframe, but not necessarily of the same crime type. VALCRI even searches for possible associations between unconnected data to compare solved and un-solved crimes, which can prove very handy in quickly generating a list of potential suspects. Every aspect of VALCRI was designed with user-friendliness and efficiency in mind. The interaction design, for instance, is based on tactile reasoning – the direct manipulation of information objects in the user interface.

The data access control security software specifies which faces a user can or cannot see, whilst video anonymization blurs out the faces of those specified.

http://valcri.org

P-REACT - Petty cRiminality diminution through sEarch and Analysis in multi-source video Capturing and archiving platform GA 607881/FP7-SECURITY

FP7-SEC-2013 has identified this need and requires low cost technology based solutions that reduce criminal activity and at the same time meet the needs and financial expectations of the communities, citizens and businesses. In response to the above issue P-REACT proposes to research and develop a sensor data (video and motion) capturing and archiving network/platform that allows the protection of small businesses from petty crimes. It is based on low cost components and built in capabilities (sensors and embedded systems) interconnecting using established and emerging technologies, such as Digital Subscriber Lines and Cloud computing.

The basic idea is to install low-cost cameras and smart sensors in the small business' premises, that are networked directly to, one or more, Cloud-based, Data Centers, where their activity is continuously monitored and recorded. A potential incident detected by sensors installed in a specific store may also trigger neighbour sensors installed in other premises near the incident in order to provide the best coverage possible in terms of data gathering.

http://p-react.eu/

AirBrush - A fast non-intrusive vapour detection system that rapidly identifies explosives in public areas GA 811977/H2020

The Eye on Air solution is a fast non-intrusive screening system for detecting explosive materials in public areas. The key innovation lies in an ultra-compact Ion Mobility Spectrometry (IMS) sensor, capable of detecting any kind of explosives as required by the European Civilian Aviation Conference (ECAC) within 2-5 seconds. The first application of the IMS technology will be AirBrush, a shoe-specific explosive vapour detection system for airports. AirBrush is the first effective shoe-specific explosive detection system, enabling seamless and quick screening of 100% passengers while significantly cutting waiting time in line and operational costs for security.

The overall objective of AirBrush innovation project is to optimize the AirBrush design and validate its performance through pilot test with NCTV at Schiphol Airport (one of the largest airport in Europe) in order to obtain relevant certification and credibility.

www.eyeonair.nl

INACHUS - Technological and Methodological Solutions for Integrated Wide Area Situation Awareness and Survivor Localisation to Support Search and Rescue Teams GA 607522/FP7-SECURITY

Crisis incidents result in difficult working conditions for Urban Search-and-Rescue (USaR) crews. INACHUS aims to achieve a significant time reduction and increase efficiency in USaR operations by providing:

a. Simulation tools for estimating the locations of survival spaces (after a structural collapse) and identify the location of survivors for different construction types and building materials
b. Decision and planning modules for advanced casualty and damage estimation that will be based on input coming from airborne and ground-based laser-scanning and imaging data
c. Integration of i) existing and novel sensors (electromagnetic, vision, chemical) for detecting and high-accurate localisation and ii) mobile phones signals for estimating the number of the trapped humans
d. A snake robot mechanism (integrated with the sensors) to penetrate inside the rubble to locate more accurately trapped victims
e. A robust, resilient and interoperable communication platform to ensure that the sensors data can reach the command centre
f. Enhanced data analysis techniques and 3-D visualization tool of the mission place to be operated by the crisis managers and the decision makers. A suitable decision support system will be used for planning & managing complex USaR operations
g. System Integration of all the aforementioned software and hardware subcomponents (INACHUS platform)
h. Contribution to standards: interaction with international organizations and public authorities in the fields of USaR, through an early defined and developed User Group, to ensure strong links with the user communities and standardisation bodies
i. Consideration of societal impacts and legal/ethical issues of the proposed solution at the onset of the project feeding into the technical solutions
j. Numerous field and simulated tests properly designed and executed for presenting the capabilities of the INACHUS integrated platform

k. appropriate training package and extensive training courses
INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS (CLOSED PROJECT)

AUGGMED - Automated Serious Game Scenario Generator for Mixed Reality Training GA 653590/H2020

The aim of AUGGMED is to develop a serious game platform to enable single- and team-based training of end-users with different level of expertise from different organisations responding to terrorist and organised crime threats. The platform will automatically generate non-linear scenarios tailored to suit the needs of individual trainees with learning outcomes that will improve the acquisition of emotional management, analytical thinking, problem solving and decision making skills. The game scenarios will include advanced simulations of operational environments, agents, telecommunications and threats, and will be delivered through VR and MR environments with multimodal interfaces. This will result in highly realistic training scenarios allowing advanced interactivity while encouraging security staff and first responders to engage and actively participate in the training process. In addition, the AUGGMED platform will include tools for trainers enabling them to set learning objectives, define scenarios, monitor training sessions, modify scenarios and provide feedback in real-time, as well as evaluate trainee performance and set training curricula for individual personnel in the post-training session phase. Finally, the platform will be offered in affordable and cost-effective Modes including Basic Mode (low VR fidelity and interactivity through mobile devices), Intermediate Mode (immersive multimodal VR) and Full Mode (immersive multimodal MR On-Site).

http://www.auggmed-project.eu/

SURVANT - SURveillance Video Archives iNvestigation assistant GA 720417/H2020

All around the world, organizations and agencies deploy video surveillance to monitor and protect property and public infrastructure, driven by various factors like increasing crime rate, security threats, terrorism acts and even monitoring of law enforcement. The influx of surveillance footage from a growing number of cameras operating at higher resolutions, such as HD, coupled with the desire to increase the retention time of that footage is exploding the volume of the footage available. Organizations that have invested heavily in surveillance infrastructure are keen to exploit it for the automation of surveillance procedures using video analytics solutions. SURVANT will deliver an innovative system that will collect the relevant videos from heterogeneous repositories, extract video analytics, enrich the analytics using reasoning and inference technologies, and offer a unified search interface to the user. An intuitive interface with a relaxed learning curve will assist the user create accurate search queries and receive the results using advanced visualization tools. Ethical management of personal data collected from surveillance videos is integrated in the system design.

SURVANT is the follow up of the research project ADVISE (GA 285024), co-financed by EU in the FP7 Work programme in the SEC-2011 call. It intends to market uptake the results achieved in ADVISE and prove the final system at operational environment (TRL9). The market opportunity has been confirmed during the ADVISE project demonstration workshops, where end-users were enthusiastic about the functionality of the prototype presented and some initial interest for purchasing the system was declared. Law Enforcement Agencies (LEAs), critical infrastructure operators and private security organizations are the primary market targets of this action. However, SURVANT pleads to explore new markets that share common needs.

https://www.eng.it/

EXPEDIA EXplosives PrEcursor Defeat by Inhibitor Additives GA 604987/FP7-SECURITY

The objectives of the EXPEDIA project are both to inhibit some frequently used explosive precursors and to increase the knowledge about “garage chemistry”. With this we mean, increasing the understanding of how terrorist’s create homemade explosives (HME), what chemicals they start from and where they find them in

the open market. But also, to increase the understanding of how easily a HME can be created, what basic equipment is necessary and what chemical knowledge is needed by the terrorist.

The output from EXPEDIA will increase the security of the citizens in Europe both in the sense that chemical inhibition will reduce/ limit or at least make it much harder for terrorists to create HMEs from readily available chemicals. Understanding the terrorist perspective regarding HME production, will directly give input to both first responders and European legislators.

As one of the output EXPEDIA will create A European guide for first responders with basic instructions on how to interpret findings on a crime scene when suspected bomb factories have been encountered.

In order for European legislators to carry out right work in the fight against terrorism, access to accurate data and an in-depth understanding of the characteristics of HMEs and various formulations thereof is of crucial importance. EXPEDIA will feed its produced information about HMEs directly to these groups via appropriate channels.

Finally, EXPEDIA will research for solutions to prevent the misuse of some explosive precursors that have not yet been investigated within the FP7 research programme. The inhibition of these precursors will be closely linked to feasibility and implementation cost studies as well as to toxicology studies. The solutions should be environmentally friendly and economically defendable in order to be able to be implemented into precursors that are produced in large quantities today.

Coordinated by:TOTALFORSVARETS FORSKNINGSINSTITUT Sweden

VICTORIA Video analysis for Investigation of Criminal and TerrORIst Activities GA 740754/ H2020

Video recordings have become a major resource for legal investigations. Since no mature video investigation tools are available and trusted by LEAs, investigators still need to carry out the analysis of videos almost exclusively manually. Current practices are too resource intensive to handle the yet huge and steadily increasing volume of videos that need to be analysed after crimes and terrorist acts. The consequence is that LEAs cannot analyse all available videos because of the huge effort needed, and the extraction of first clues from videos after a terrorist attack takes more time. VICTORIA will address this need and deliver a Video Analysis Platform (VAP) that will accelerate video analysis tasks by a factor of 15 to 100 (depending on the use case), while providing very reliable results. To achieve this, VICTORIA will 1) develop a set of TRL-6 video analytics selected for their relevance in video investigation related to crimes and terrorist acts, 2) increase significantly the usability of delivered tools by involving LEAs directly in all stages of the development process, from specifications, over assessment of several VAP prototype versions, up to field trials in LEA operational conditions, 3) create an ecosystem around an open VAP concept, that will facilitate sustainable innovation and market growth for video investigation products, 4) train LEA investigators in the use of the VAP, 5) ensure that VICTORIA activities and results meet EU Legal-Ethical-Privacy rules. The VAP will have a scalable architecture based on big data technologies, feature new user interface paradigms allowing complex semantic investigation queries and 4D crime scene reconstruction, be adaptable to specific user needs, and be future proof thanks to an open analytics plug-in feature, based on standardized interfaces and open to third party suppliers. The consortium includes 4 LEAs, 6 renowned research groups, 2 SMEs and 2 industrial companies, world-leaders in security markets.
In view of the needs and challenges described above and the absence of a robust technical solution, VICTORIA aims at creating a real breakthrough regarding functionality and usability of video analysis tools used for legal investigations. To achieve these aims, the VICTORIA project will address the following five specific objectives:
- Develop a TRL-6 video analysis technology that will boost the LEAs' video investigation capacity
- Increase significantly the usability of video analysis tools for legal investigations
- Create a business model and ecosystem allowing the video investigation field to grow and prosper
- Train LEA investigators in the use of advanced video investigation tools
https://www.victoria-project.eu

STAIR4SECURITY - STANDARDS, INNOVATION AND RESEARCH FOR SECURITY GA 853853/ H2020

A wide range of security threats including man-made and natural risks can result in disruptive events having serious consequences for societal and citizen security. Both, public and private stakeholders require adequate solutions in organization, procedures and technological capabilities to be able to respond timely and effectively. Thus, there is a need to develop specific standards to enable the various public and private organizations within Europe, being local, national, European or international to be effectively coordinated ensuring as much as possible a smoothly cooperation before, during and after a disruptive event. The main objective of this proposal is to propose a collaborative platform as single entry point of information on the security sector coming mostly from research activities allowing a better governance of standardization needs in the Disaster Resilience and Chemical Biological Radiological Nuclear and Explosive (CBRN-E) sectors. The aim of the platform is to permit a better overview of current and new projects being at, national, European or International level; ensuring more coordination between all stakeholders and responding more efficiently and timely to the critical needs following an agreed strategic vision and identified priorities. Besides ensuring the necessary partnering network, the project will review the necessary tools and mechanisms including the CEN and CENELEC Workshop Agreement (CWA) process and a fast-track procedure to adopt, if market relevant, a CWA or any other deliverable or reference document e.g. TS and TR into a consensus standard (EN). Possibilities and conditions to include classified information in a non-consensus standard (CWA, TS or TR) will also be explored.

https://cordis.europa.eu/project/rcn/220087

RED-Alert - Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing GA 740688/H2020

The RED-Alert project will bring data mining and predictive analytics tools to the next level, developing novel natural language processing (NLP), semantic media analysis (SMA), social network analysis (SNA), Complex Event Processing (CEP) and artificial intelligence (AI) technologies. These technologies will be combined for the first time and validated by 6 law enforcement agencies (LEAs) to collect, process, visualize and store online data related to terrorist groups, allowing them to take coordinated action in real-time while preserving the privacy of citizens. The RED-Alert solution will outperform state-of-the-art solutions in terms of number of languages supported, privacy preserving capabilities, usability, detection performance, real-time capabilities and integration capabilities. The RED-Alert approach combines for the first time the CEP methodology with NLP/SMA and SNA applications in the context of social media data analytics, transforming (unstructured) social media data into (structured) events enhanced by semantic attributes. For example, a tweet will be an event consisting of content (expressed as NLP features e.g. concepts, sentiment, entities, etc.) and context (time and the author including SNA features e.g. number of followers, number of links, etc.). Turning unstructured social media data into structured events is key, as it allows the system to use (event) rules (event temporal logic, event logic patterns, even counting, absence of events) to infer insights or create alerts in real-time. The project impact is supported by the participation of Europol and specific dissemination activities around the World Counter Terrorism Summit, organized by one of the partners. The total requested EC funding is 5M Euros and the project duration 36 months.

www.redalertproject.eu

Arcopter The Game Changer Free-wing VTOL Drone for Commercial and Governmental Missions GA 816552 H2020

Drones, technically known as Unmanned Aerial Vehicles (UAVs), are evolving beyond their military origin shaping brand new operating models and becoming a powerful tool for a wide range of commercial application, such as agriculture, infrastructure, security, media and entertainment, and telecommunications, resulting to a global market size of €12bn by 2020. Nevertheless, their widespread implementation is restrained by the limitations of commercialized technologies [multi-rotors, fixed-wings and Vertical Take-off and Landing (VTOL) fixed-wings] in flight range, usability or instability and inaccurate VTOL under windy conditions.

ARcopter aims to revolutionize the commercial drone's market by introducing the first UAV that combines fully autonomous operation, accurate Vertical Take-Off and Landing (VTOL) and capability to operate in windy conditions. Based on our revolutionary Loose WingTM control system, we offer a drone able to VTOL like a copter and fly horizontally as efficient as an airplane. ARcopter can fly for 2.5 hours (up to 3 times more flight duration) and 150 km flight range and do accurate landings relative to the ground in 55km/h wind speeds when the best that competitors can offer is 35km/h. All the above achieved by a fully autonomous operation carrying a variety of payloads (cameras) based on the customer's needs and application. We initially target 1) Oil and gas companies, voltage network owners, wind turbine and railway operators for infrastructures inspection and monitoring, 2) Individual farmers and cooperatives for precision farming and 3) Governmental agencies firefighters police, border patrol, coastguard for Homeland Security (HLS) and Public Safety. Its breakthrough and game changer characteristics providing safety, efficiency and cost benefits for its users will constitute drones for large scale commercial and governmental purposes a common tool.

https://www.colugo-sys.com/

CURSOR Coordinated Use of miniaturized Robotic equipment and advanced Sensors for search and rescue OpeRations GA 832790 H2020

The CURSOR proposal aims at developing new and innovative ways of detecting victims under debris. This includes the coordinated use of miniaturized robotic equipment and advanced sensors for achieving significant improvements in search and rescue operations with respect to (a) the time used to detect trapped victims after a building structure has collapsed, and (b) an informed and accelerated decision making by first responders during rescue operations allowing for the deployment of expert personnel and, in particular for operations in hazardous environments, suitable equipment at prioritized locations. CURSOR is proposing a system consisting of several integrated technological components. It includes Unmanned Aerial Vehicles (UAVs) for command & control, 3D modelling and transportation of disposable miniaturized robots, that are equipped with advanced sensors for the sensitive detection of volatile chemical signatures of human beings. Information and data collected are transferred in real time to a handheld device operated by first responders at the disaster site.

https://cordis.europa.eu/project/rcn/222585

DARWIN Expecting the unexpected and know how to respond GA 653289 H2020

Compared to the past, recent disasters challenge society in terms of dealing with the unexpected, large scale, highly interconnected society and trans-boundary nature of events involving different countries, many private and public stakeholders and high expectations from the citizens. The DARWIN project addresses the improvement of responses to expected and unexpected crises affecting critical infrastructures and social structures. It covers the management of both manmade events (e.g. cyber-attacks) and natural events (e.g. severe weather). The overall objective and main result is the development of European resilience management guidelines. These will improve the ability of stakeholders to anticipate, monitor, respond, adapt, learn and evolve, to operate efficiently in the face of crises. All results of the project are public to facilitate their use. The target beneficiaries of DARWIN are crisis management actors and stakeholders

responsible for public safety, such as critical infrastructures and service providers, as well as community groups.

The main objectives and results of the project were:

• Make resilience guidelines available for a particular critical infrastructure operator by developing and adapting the DARWIN resilience management guidelines (DRMG) to health care and air traffic management domains;

• Enable use of resilience guidelines in non-crisis situations supporting training and evaluation by delivering handouts to facilitate workshop, modules for a Master programme, material for lectures and proposing prototypes for simulation and serious games;

• Facilitate evolution of the guidelines proposing DARWIN Wiki as a knowledge management platform and by involving practitioners, that can evolve and integrate their needs and experiences;

• Establish a Community of Resilience and Crisis Practitioners (DCoP) by proposing highly interactive virtual and face to face activities to co-create and facilitate adaption and adoption of the DRMG. At peak the DCoP forum included 173 members from 25 countries;

• Build on lessons learned in the area of resilience by establishing a link between resilience capabilities and existing approaches and practices relevant for specific domains. This includes shared views from experts and practitioners from different domains;

• Carry out two pilot exercises that apply project results in two domains, the project performed more exercises than planned. Four pilot exercises were conducted addressing health care, air traffic management including cascade effects to other domains. Moreover, a small-scale evaluation was performed addressed highways. The evaluation actively involved 247 practitioners from 22 countries.

• Establish activities that will lead to project results being adapted to and later adopted by practitioners, workshops, webinars and presentations involving DCoP members have been performed. A white paper on resilience management was produced by five European projects with major contributions by the DARWIN consortium. Contribution to standardisation with knowledge from the project have been provided.

https://h2020darwin.eu

QROC - Quick response for Operational Centres coordinated by DITSS

This project shares needs and best practices and increases the foresight regarding (the uptake of) new innovative technologies for operational centers to improve the public protection. To that aim, the QROC project will build a communication capability between the Law Enforcement National Operation Centers (NOC) to share quickly and secure operational data across borders regarding terrorist threats to protect the public. Tangible results based on continuous testing of a new Capability Package (CP), self-assessment tool for NOCs, demonstration of and innovative technologies, along with education and practical training via a series of tabletop exercises will increase the efficiency, and the capacity of NOCs. This project is an initiative of the Core group of the European Network of Law Enforcement Technology Services (ENLETS).
Expected impact:
1. Increasing the coordination and collaboration of National Operation Centers (NOC) to quickly anticipate and respond to terrorist threats.
2. Implementing and testing a new Capability Package (CP) in National Operation Centers (NOC).
3. Paving the ground for a new era related to information sharing and data handling.
Outcomes:
1. Implementation of a technical Pan European solution that will connect the member states Operation Centers and will provide them with a swift and secure communication mechanism to exchange and

disseminate operational data pre- in and after an attack. This outcome will be achieved with the support of EU Lisa, the large-scale ICT agency, avoiding any duplication of EU systems.
2. An increased awareness of technology which can enrich the technological capabilities of Operation Centers to collect, store, process and analyse data, such as video and social media messages to protect the public
3. Training and education of staff of Operation centers based of innovative use cases to increase skills, knowledge and performance related to a terrorist and/or CBRN attack.
DUTCH INSTITUTE FOR TECHNOLOGY SAFETY & SECURITY

ANNEX II. TECHNOLOGIES

This annex contains a list of technologies for mitigating vulnerabilities in the protection of public space. The technologies are summarised in a table, which includes details regarding the following aspects of each technology (columns in the table). The technologies are sorted by technology category (the first column).

Technology category (to assist the councils in narrowing down the technology options):

1. ICT (for communicating, storing, analysing and protecting information)
   Examples: WiFi, IoT, Encryption, VPN
2. Sensors (for detection, identification, localisation, tracking)
   Examples: cameras, facial recognition, acoustic sniper localisation
3. Actuators (for warning, intercepting, eliminating)
   Examples: sirens, anti-drone drones, HPM vehicle stopping
4. Physical measures (for controlling access, impeding an attack, protective materials)
   Examples: tourniquets, portable rising steps, bomb blast window film
5. Methods (procedures, best practices, standards, etc)
   Examples: ISO 31000 Risk Management

Technology description, which could include:

- main technology principle
- strengths and weaknesses

Threat types (taken from EU VAT):

1. Firearms attack - small calibre pistol or semi/full-automatic rifle (e.g. AK47)
2. Sharp object attack - knifes, machete, other sharp and blunt objects
3. Vehicle Attack - use of vehicle as a weapon by ramming large crowds
4. IED (explosives) - left/concealed in objects or goods (based on home-made or commercial explosives)
5. PBIED (explosives) - explosives concealed on a person (suicide or carrier)
6. UAVIED (explosives) - explosives delivered by a remote-controlled airborne device
7. VBIED (explosives) - explosives concealed inside a vehicle (or its cargo)
8. Chemical attack - threat object concealed in goods or carried items (e.g. canister or UAV dispensed)
9. Biological attack - threat object concealed in goods or carried items (e.g. canister or UAV dispensed)
10. Radiological attack - threat object concealed in goods or carried items (e.g. canister or UAV dispensed)

Threat phases:

1. Initial Target Identification
2. Operational Planning
3. Pre-Attack Preparations
4. Execution
5. Post-Attack/Escape

Technology use categories (taken from EU VAT):

1. ALERT - used for alerting public (e.g. sirens, texting service)
2. SURVEIL - used for situational awareness (e.g. cameras, social media tools)
3. RESPOND - used for responding to an attack (e.g. security personnel, non-lethal weapons)
4. PROTECT - used to protect assets (people, buildings, infrastructure)
5. DETECT - used for detecting a weapon or weapon use (e.g. entry scanning equipment)
6. OVERCOME - used for overcoming a sudden vulnerability (e.g. extra concertina wire)
7. IMPROVISE - created on the spot from available means (e.g. use police vehicle as a road block)
8. RESTRICT - used for restricting public access (e.g. safety barriers)
9. ADAPT - used for changing circumstances (e.g. moving assets to a safer location)
10. OTHER

Technology common evaluation criteria:

1. Physical (weight, size, etc)
2. Cost (purchase, hire, personnel, maintenance, etc)
3. Utilisation (readiness, acquisition time, deployment time, interfacing, etc)
4. Compliancy (privacy protection legislation, data protection directives, standards, etc)
5. Performance (detection rate, failure rate, reaction time, intruder delay time, etc)
6. Other

Products/suppliers:

- Product names and types
- Product manufacturer or suppliers

This report was funded by the European Union's Internal Security Fund — Police under grant agreement n° 815356

Tech category	Tech description	Threat type	Threat phase	Tech use	Tech criteria	Products/suppliers
ICT technology	Detection of deviant behaviour online (by combining data science (how to extract and model online behaviour) and social science (which behaviours to address))	all	Initial target identification	Surveil	Performance (detection rate)	n/a
	Vulnerability assessment of individuals before the fact (for example, Multi-Agency Vulnerability Assessment Support Tool (MAVAST))	all	Initial target identification	Surveil	Performance (accuracy, at face value as data are largely absent)	Multi-Agency Vulnerability Assessment Support Tool (MAVAST): supports multi-agency teams (for example, police, justice, municipality, social work) in identifying the level of vulnerability of an individual to radicalise in a violent way (by TNO for H2020 Pericles)
	GIS system for geographical information	all	Execution / post-attack/escape	Surveil / respond / protect /	Performance	n/a

				detect / improvise		
	Video analytics	all	Initial target identification / execution / post-attack/escape	Surveil / respond / protect / detect	Performance	n/a
Sensor technology	Weapon detector (DEXTER)	Fire arms attack	Pre-attack	Surveil / detect / protect	Performance (detection rate)	n/a
	Explosive detector (DEXTER)	PBIED	Pre-attack	Surveil / detect / protect	Performance (detection rate)	n/a
	Automatic vehicle behaviour and threat detection (SASSSISLAN)	Vehicle Attack	Pre-attack	Surveil / protect	Performance (detection rate)	n/a
	Automatic person behaviour and threat detection (SASSSISLAN)	Sharp object attack / PBIED	Pre-attack	Surveil / protect	Performance (detection rate)	n/a
	Automatic aggression detection	Sharp object attack	Pre-attack / execution	Surveil / protect	Performance (detection rate)	n/a
	Person re-identification to avoid next attack (DEXTER)	PBIED	Post-attack / Pre-attack (next)	Surveil / detect / protect	Performance (detection rate)	n/a

Automatic crowd behaviour and threat detection (SASSSISLAN)	Sharp object attack	Pre-attack / execution	Surveil / protect	Performance (detection rate)	n/a
mmw-portals (≈30-300 GHz)	Fire arms, sharp object, PBIED, chemical, biological & radiological attack	Execution	Detect	anomaly detection, slow (person by person)	L-3 Provision, Rohde & Schwarz QPS200, Smiths Echo, Nuctech
mmw walk-through (≈30-300 GHz)	Fire arms, sharp object, PBIED, chemical, biological & radiological attack	Execution	Detect	anomaly detection (several 100 persons/h)	Evolv Edge, APSTEC HSR, R&S (Camero) Easycheck
radar/microwave (≈3-30 GHz)	Fire arms, sharp object, PBIED, chemical, biological & radiological attack	Execution	Detect	anomaly detection large distance	Rapiscan Counterbomber
THz/IR cameras	Fire arms, sharp object, PBIED, chemical, biological & radiological attack	Execution	Detect	anomaly detection difficult image interpretation	THz - no COTS equipment on the market IR – ELBIT IR camera
X-ray backscatter persons	Fire arms, sharp object, PBIED, chemical, biological & radiological attack	Execution	Detect	forbidden for use in public in Europe – ionising radiation	Rapiscan (discontinued product)

X-ray transmission persons	Fire arms, sharp object, PBIED, chemical, biological & radiological attack	Execution	Detect	forbidden for use in public in Europe – ionising radiation	Smiths Detection B-scan
X-ray transmission belt systems	Fire arms, sharp object, IED, chemical, biological & radiological attack	Execution	Detect	checkpoint necessary, slow (bag by bag), ATR possible for explosives, guns and knives	many commercial systems available
X-ray backscatter for cars	Fire arms & VBIED attack	Execution	Detect	covert: needs close proximity to car (drive by), image difficult to interpret, Mobile Portal solution possible, checkpoint situation, driver has to leave the car	Rapiscan (many products)
Explosive vapour Detection – High Volume Sampling (HVS)	IED, PBIED & VBIED attack (potentially chemical attack)	Execution	Detect	not all explosives can be detected, detection rate depends on circumstances (eg temperature), needs time (1-30 minutes), sampling device is portable, detection device is large and expensive, detector usually mass spectrometer based technology	SEADM, Karsa

Explosive vapour Detection – Direct Sampling	IED, PBIED & VBIED attack (potentially chemical attack)	Execution	Detect	Less sensitive than HVS, lower DR, handheld, limited use, many technology sub categories	Rapiscan Mobile trace, Fido
Explosive Trace Particle detection – contact	IED, PBIED & VBIED attack (potentially chemical attack)	Execution	Detect	contact with object necessary (swab), very sensitive equipment mostly Ion Mobility Spectrometry (IMS) based, but also other technologies success depends on skill operator	Bruker, Nuctech, Rapiscan, Smiths Detection, L-3 and others
Explosive Trace Particle detection – non-contact	IED, PBIED & VBIED attack (potentially chemical attack)	Execution	Detect	Mostly Raman-effect based technology, use of laser, eye-safety is an issue when use in public. Proximity measurements (<2 cm) are mature, longer distance (up to several meters) less mature, also bulk detection possible up to 40 m for some explosives (low TRL), line of sight necessary	Thermo Fisher (True/First defender), ALAKAI, ENEA (prototype, low TRL)
Walk Through Metal Detection	Fire arms, sharp object & vehicle attack	Execution	Detect	checkpoint necessary, only works if threat contains metal	Ceia, Rapiscan, Garret
Hand held Metal Detector	Fire arms, sharp object & vehicle attack	Execution	Detect	depends on skill operator, only works if threat contains metal	Ceia, Rapiscan, Garret

Explosive Detection Dogs	IED, PBIED & VBIED attack (potentially chemical attack)	Execution	Detect	versatile use, performance varies from dog to dog and in time, expensive	mostly police, military, though commercial parties do exist (PMT, Twickelerveld)
Pat down	Fire arms, sharp object, PBIED, chemical, biological & radiological attack	Execution	Detect	often used as alarm resolution, invasive, time consuming, depends on skill of the screener and cooperation of the subject	Screeners can be supplied by private security companies (G4S, Securitas)
Visual inspection of bags, cars, etc.	Fire arms, sharp object, PBIED, chemical, biological & radiological attack	Execution	Detect	often used as alarm resolution, invasive, time consuming, depends on skill of the screener and cooperation of the subject	Screeners can be supplied by private security companies (G4S, Securitas)
Detection of deviant behaviour offline (for example, security questioning, distinguishing psychiatric patient from terrorist (Rapid Observation of Psychological Disorders (ROPD) tool))	all	Execution	Surveil	Performance (detection rate)	Rapid Observation of Psychological Disorders (ROPD) tool: translation of a psychopathology diagnostic tool for healthcare professionals into manageable questions with everyday terms for safety professionals (TNO)
Use of animals as *sensor* (for example,	all	Execution	Surveil / respond /	Readiness / Performance	n/a

emotions, stress level, use of substances, presence of explosives, and establishing identity)			detect / restrict		
Risk assessment of individuals on the spot (i.e., stress assessment)	all	Execution	Respond / detect	Performance (accuracy)	Rapid Resilience Scan: estimates the effects of behavioral measures on a target. The RRS is being developed for measuring stress and resilience in a criminal context (by TNO)
Vulnerability assessment of individuals before the fact (for example, Multi-Agency Vulnerability Assessment Support Tool (MAVAST))	all	Initial target identification	Surveil	Performance (accuracy, at face value as data are largely absent)	Multi-Agency Vulnerability Assessment Support Tool (MAVAST): supports multi-agency teams (for example, police, justice, municipality, social work) in identifying the level of vulnerability of an individual to radicalise in a violent way (by TNO for H2020 Pericles)
Automatic sprinkler system	IED, PBIED, UAVIED & VBIED attack	Execution	Respond / protect / overcome	Performance	n/a

	Drones with sensor	all	Initial target identification / execution / post-attack/escape	Surveil / respond / detect	Performance (detection rate, accuracy)	n/a
Actuator technology	Influence attacker in communication (for example, negotiation strategies, security questioning, communication skills)	all	Execution	Respond	Performance	Security Questioning Protocols
	Deception of attacker (for example, distract (i.e., slow down) by unexpected noises or physical barriers)	all	Execution	Respond	Readiness / Performance	Psychological Intervention Guide for PBIED attacks: multidimensional matrix of significant aspects of PBIED in crowd, facilitates sense making in using softer methods to delay/protect (by TNO, for FP7 SUBCOP)
	Loudspeakers	all	Execution / post-attack/escape	Alert	Physical	Many available
	Lights on pathways (maybe	all	Execution / post-attack/escape	Respond	Physical / readiness / performance	n/a

in combination with sensor)					
Crowd control (for example, influence techniques or use of social media)	all	Execution	Alert / protect / restrict	Readiness / Performance	n/a
Non lethal weapons (acoustic, electroshock, et cetera)	Fire arms, sharp object, PBIED attack	Execution	Pre-attack preparations	Physical / cost	n/a
Weapons to stop the terrorist during the attempted attack	Fire arms, sharp object, vehicle, PBIED attack	Execution	Pre-attack preparations	Cost / compliancy	n/a
Intervention to stop the terrorist during the attempted attack	Fire arms, sharp object, PBIED attack	Execution	Pre-attack preparations	Other: effectiveness	n/a
Use of animals as *actuator* (for example, influencing behaviour in an overt manner (for example intimidation) and a covert manner)	all	Execution	Surveil / respond / detect / restrict	Readiness / Performance	n/a

Physical technology	Influence attacker physically (for example, intimidate, Less Lethal Weapons (sound, vision))	all	Execution	Respond / restrict	Readiness / Performance	Psychological Intervention Guide for PBIED attacks: multidimensional matrix of significant aspects of PBIED in crowd, facilitates sense making in using softer methods to delay/protect (by TNO, for FP7 SUBCOP)
	Physical barriers that are flexible or permanent	Vehicle attack	Pre-attack preparations	Protect	Readiness / performance	Many available
	Urban layout with bollards, planters, et cetera	Vehicle, VBIED attack	Execution	Protect	Other: impact, architectural looks	n/a
	Reduce the loading on a building by using landscape design	VBIED attack	Execution	Protect	Cost and other: effectiveness	n/a
	Design of roads to prevent the impact of vehicles with a high speed	Vehicle, VBIED attack	Execution / Post-Attack/Escape	Protect	n/a	n/a
	Prevent crowded places with	all	Execution	Protect	n/a	n/a

environment design					
Temporary measures – vehicle barriers, checkpoint, road block	Vehicle, VBIED attack	Execution	Protect	Physical, cost and other: impact on normal operations	n/a
Permanent measures – security gate, (blast resistant) fencing, bollards….	Vehicle, VBIED attack	Execution	Protect	Physical, cost and other: impact on normal operations	n/a
Façade design (include the window and door anchors)	IED, PBIED, UAVIED, VBIED attack	Execution	Protect	Physical / cost	n/a
Explosion resistant glazing	IED, PBIED, UAVIED, VBIED attack	Execution	Protect	Physical / cost	n/a
Bullet proof glazing	Fire arms attack	Execution	Protect	Physical / cost	n/a
Prevent progressive collapse	IED, PBIED, UAVIED, VBIED attack	Execution	Protect	Physical / cost	n/a
Prevent roof objects like lightning, panels	IED, PBIED, UAVIED, VBIED attack	Execution	Protect	Physical / cost	n/a

	to fall on the people					
	Provide a safe place for shelter	Fire arms, sharp object attack	Execution	Protect	Physical / cost	n/a
	Products to mitigate or reduce the explosion effects like blast container (place them around the threat) to isolate the threat	IED, PBIED attack	Execution	Protect	Other: (It might be effective to protect the surrounding, but also has side effects. E.g. additional risk for EOD)	n/a
	Personal protection (vest, helmet, gear) to the first responders and security personnel	Fire arms, sharp object attack	Pre-attack preparations / Execution	Respond	Physical / cost / performance	n/a
	Bomb suit (Explosive ordnance) of the first responders and security personnel	IED, PBIED, UAVIED, VBIED attack	Execution / Post-Attack/Escape	Respond	Physical / performance	n/a
Method technology	Increase resilience LEOs (for	all	Pre-attack preparations	Other (or all)	Readiness	Training and monitoring by TNO for Police and MinDef

example, training, monitoring)					
Trainings to enhance LEO capabilities (for example, flexibility, communication skills)	all	Pre-attack preparations	Other (or all)	Performance (measured increase in capabilities)	Trainings by TNO for Police and MinDef
Enhance multiparty decision making (for example, reducing bias, improving collaboration)	all	all	Other (or all)	Readiness / Compliancy	Multidisciplinair Interactie Raamwerk by TNO for Flood Control 2015 (http://digitalpages.tno.nl/mirror/page/1)
Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide November 2015	Fire arms	Execution	SURVEIL, RESPOND, PROTECT, DETECT	Readiness / Compliancy	DHS website
Security and Resiliency Guide: Counter-Improvised	IED, PBIED, UAVIED, VBIED (explosives)	Pre-attack preparations, Execution	SURVEIL, RESPOND,	Readiness / Compliancy	DHS website (https://www.dhs.gov/publication/security-and-

Explosive Device (C-IED) Concepts (including for events and sports venues)			PROTECT, DETECT		resiliency-guide-and-annexes)

Table 12 List of technologies for the protection of public spaces and related suppliers

This report was funded by the European Union's Internal Security Fund — Police under grant agreement n° 815356

END OF DOCUMENT