Grant number: 883286
Project duration: Sep 2020 – Aug 2022
Project Coordinator: Joe Gorman, SINTEF

Horizon 2020: Secure societies
SU-INFRA02-2019
Security for smart and safe cities, including for public spaces
Project Type: Innovation Action

http://www.impetus-project.eu

IMPETUS Project Deliverable: D1.2

Requirements for public safety solutions

Dissemination Status: Public

Editor: Matthieu Branlat (SINTEF)

Authors: Matthieu Branlat, Martina Ragosta, Stine Skaufel Kilskar, Ravi Borgaonkar, Andrea Vik Bjarkø, Maria Vatshaug Ottermo, Tor Olav Grøtan, Joe Gorman (SINTEF); Sandrine Bayle, Gilles Dusserre, Joaquin Garcia-Alfaro, Keren Saint-Hilaire (IMT); Axelle Cadiere (UdN); Claudio Ardagna, Michelangelo Ceci, Paolo Mignone, Costantino Mele, Donato Malerba, Marco Anisetti, Alessandro Balestrucci (CINI); Paolo Mocellin, Matteo Bottin, Chiara Vianello, Silvio Cocuzza, Giulio Rosati, Giuseppe Maschio (UPAD); Radu Popescu, Andrei Ogrezeanu, Dragos Trifan, Gabriel Nicola (SIV); Rafal Hrynkiewicz, Johan de Heer (THA); Joe Levy (CINEDIT); Berta Biescas, Joaquín Luzón Tuells (INS); Tobias Traebing (XM); Bruno Bonomini, Giulia Canilli (CPAD); Ian Simon Gjetrang, Lars Ole Grottenberg, Osman Ibrahim, Juan Cabrera, Eirik Bærulfsen (OSL); Mišo Mudrić, Jelena Radosevic, Krunoslav Katic, Filip Dragovic (ISP); Thomas Robertson, George Markowski, Gbenga Morenikeji, Greg Swick (TIEMS), Alberto Da Re, Stefano Gallinaro (UNI)

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

Grant number:	883286
Project duration:	Sep 2020 – Aug 2022
Project Coordinator:	Joe Gorman, SINTEF

Horizon 2020: Secure societies
SU-INFRA02-2019
Security for smart and safe cities, including for public spaces
Project Type: Innovation Action

About IMPETUS

IMPETUS (Intelligent Management of Processes, Ethics and Technology for Urban Safety) is a Horizon 2020 Research and Innovation project that provides city authorities with new means to improve the security of public spaces in smart cities, and so help protect citizens. It delivers an advanced, technology-based solution that helps operational personnel, based on data gathered from multiple sources, to work closely with each other and with state-of-the art tools to detect threats and make well-informed decisions about how to deal with them.

IMPETUS provides a solution that brings together:

- *Technology*: leverage the power of Internet of Things, Artificial Intelligence and Big Data to provide powerful tools that help operational personnel manage physical and cyber security in smart cities.
- *Ethics*: Balance potentially conflicting needs to collect, transform and share large amounts of data with the imperative of ensuring protection of data privacy and respect for other ethical concerns - all in the context of ensuring benefits to society.
- *Processes*: Define the steps that operational personnel must take, and the assessments they need to make, for effective decision making and coordination - fully aligned with their individual context and the powerful support offered by the technology.

Technological results are complemented by a set of *practitioner's guides* providing guidelines, documentation and training materials in the areas of operations, ethical/legal issues and cybersecurity.

IMPETUS places great emphasis on taking full and proper account of ethical and legal issues. This is reflected in the way project work is carried out, the nature of the project's results and the restrictions imposed on their use, and the inclusion of external advisors on these issues in project management.

The cities of Oslo (Norway) and Padova (Italy) have been selected as the site of practical trials of the IMPETUS solution during the project lifetime, but the longer-term goal is to achieve adoption much more widely.

The work is carried out by a consortium of 17 partners from 11 different EU Member States and Associated Countries. It brings together 5 research institutions, 7 specialist industrial and SME companies, 3 NGOs and 2 local government authorities (the trial sites). The consortium is complemented by the Community of Safe and Secure Cities (COSSEC) – a group established by the project to provide feedback on the IMPETUS solution as it is being developed and tested.

The project started in September 2020 with a planned duration of 24 months (possibly to be extended to 30 months).

For more information

Project web site:	https://www.impetus-project.eu/	
Project Coordinator:	Joe Gorman, SINTEF:	joe.gorman@sintef.no
Dissemination Manager:	Snježana Knezić, TIEMS:	snjezana.knezic@gmail.com

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

Executive Summary

Background and objectives: The central objective of this deliverable is to provide the requirements for the development of the results of project IMPETUS (platform, specific solutions, frameworks). The requirements are motivated by a background section that contains rich knowledge about public safety operations and technology. This content gives multiple perspectives on the topic central to the project, i.e., the use of technology to support public safety, and therefore serves as a source of information to facilitate learning and collaboration across partners. The development of requirements is directly related to the scope and objectives of project IMPETUS: the main ambitions of the project are related to (1) integrating mostly mature technologies for public safety in a smart city environment, and (2) producing accompanying guidance and tools to address the operational, legal and ethical, as well as cyber security aspects of the use of such capabilities. The requirements presented in this document therefore reflect these primary concerns.

Approach: An extensive investigation was conducted of the various aspects associated with technological solutions for public safety. Based mostly on an analysis of scientific literature and technical reports, but also on focus groups and a survey, this investigation includes a state of the art, a study of the perception of stakeholders and an analysis of issues and challenges (technological, operational and ethical). The content generated motivated the development of requirements. A content structure as well as a collaborative and iterative process were implemented to support the development, review and revision of the project requirements.

Results and conclusions: The rich background material of this document serves as motivation for the requirements, but also as a common source of information about all the topics covered in this very multi-disciplinary project. The requirements described here are a snapshot of a list of requirements which will keep on evolving during the life of the project, in order to improve (e.g., clarify) existing requirements and fill potential gaps. It will be used by all following WPs.

Table of Contents

Executive Summary **3**

Abbreviations and definitions **10**

1 About this deliverable **11**

1.1 Intended readership/users 11

1.2 Why would I want to read this deliverable? 11

1.3 Structure 11

1.4 Other deliverables that may be of interest 11

PART I. TECHNOLOGICAL SOLUTIONS FOR PUBLIC SAFETY IN SMART CITIES **13**

2 State of the art: technological capabilities currently implemented in smart cities **14**

2.1 Typical smart city applications 14

2.1.1 The layered vision of Smart Cities 15

2.1.2 International examples of Smart Cities 17

2.1.3 Smart Cities in Europe 18

2.1.3.1 Copenhagen, Denmark 19

2.1.3.2 London, United Kingdom 19

2.1.4 Example outside Europe: Boston, United States 20

2.2 Specific examples of public safety applications 20

2.2.1 Safe city concept and its features 20

2.2.2 Innovative solutions for safety in cities 21

2.2.2.1 Personal safety 21

2.2.2.2 Infrastructure security 22

2.2.2.3 Health security 24

2.2.2.4 Digital security 25

2.2.2.5 Applications under development, developed and implemented 26

2.3 Stakeholders of public safety solutions 26

3 Perception by stakeholders **28**

3.1 Cities: officials and managers 28

3.1.1 General conclusions of the focus group analysis 28

3.1.2 General opinions about ethical issues in Smart City technologies and sense of personal security 29

3.1.3 Personal experiences 29

3.2 Emergency and security organisations: managers and personnel 30

3.2.1 Ethics and Privacy 31

3.2.2 Technology Implementation 32

3.2.3 Other Operational Considerations 33

3.3 Population: citizens and citizen organisations 33

3.3.1 Research conducted 33

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

3.3.2 Summary of results ... 34

4 Technical issues ... 36

4.1 Security and safety solutions ... 36

4.1.1 Cyber Security ... 36

4.1.2 Communications infrastructure ... 38

4.1.3 Verification and surveillance ... 39

4.1.4 Biochemical Risk Detection ... 39

4.1.5 Gaps and challenges ... 41

4.2 Case studies and real-world incidents ... 45

4.2.1 Ransomware Attacks ... 45

4.2.2 Human performance issues ... 46

4.2.3 Electronic Communications Limitation and Lack of Interoperability ... 46

4.2.4 Biased Automatic Facial Recognition ... 46

4.2.5 Biochemical Risk Detection ... 47

4.2.6 Nation-state attacks ... 47

5 Operational issues ... 49

5.1 Intelligence ... 49

5.1.1 Redundant information and data overload ... 49

5.1.2 Access to information: darknet, social media and chat applications ... 50

5.1.3 Access to information from other intelligence agencies and disciplines ... 50

5.1.4 The challenge of providing targeted and relevant intelligence ... 51

5.2 Detection of events ... 51

5.2.1 Attentional challenges ... 51

5.2.2 Preparing for uncertainty: detection and response ... 52

5.3 Sensemaking and situational awareness ... 53

5.4 Decision-making ... 54

5.5 Intervention ... 54

5.6 Coordination across roles and organisations ... 55

5.7 Operational risks in introducing new technology ... 56

5.8 Learning from events: summary ... 57

6 Ethical and legal issues ... 59

6.1 General considerations ... 59

6.1.1 Socio-technical environment ... 59

6.1.2 Involuntary data collection and manipulation ... 60

6.1.3 Mass surveillance ... 60

6.1.4 Common good ... 60

6.1.5 Privacy and personal data ... 60

6.2 Legal analysis ... 61

6.2.1 Moral machines ... 63

6.2.2 Supervision and oversight ... 64

6.2.3 Stakeholders ... 64

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

6.3 Critical requirements and principles 64
6.3.1 Ethics guidelines for trustworthy AI 64
6.3.2 Critical requirements 65
6.3.3 Fundamental principles 65

PART II. REQUIREMENTS FOR PUBLIC SAFETY SOLUTIONS 68

7 Development of requirements 69
7.1 Development process 69
7.1.1 Core principles 69
7.1.2 Input to requirements 69
7.1.3 Process to draft, review and revise requirements 70
7.1.3.1 General organization 70
7.1.3.2 Importance of the review and revision process 71
7.1.4 Challenges in requirements development 71
7.1.4.1 Homogenisation of content 71
7.1.4.2 Remaining uncertainty: 71
7.2 Requirements format and content 71
7.2.1 Format 71
7.2.2 Fully detailed examples of requirements 75

8 Overview of requirements for the development and implementation of public safety technology . 78
8.1 Requirements for the Public safety Platform 78
8.2 Requirements for the specific Public safety Capabilities 80
8.3 Requirements for the management and processing of Smart City data 80
8.4 Requirements for the Cyber security Framework 81
8.5 Requirements for the Ethical and legal Framework 82
8.6 Requirements for the Operational Framework 82

9 Conclusions and next steps 84
9.1 Challenges and limitations in requirements development 84
9.2 Maturity of the requirements presented 84
9.3 Evolution of the requirements 84

10 References 85
10.1 State of the art: technological capabilities currently implemented in smart cities 85
10.2 Perception by stakeholders 87
10.3 Technical issues 88
10.4 Operational issues 91
10.5 Ethical and legal issues 92

APPENDICES 97

A Detailed results from survey of public perception 98
A.1 Level of familiarity with the concept of Smart Cities 98

A.2 Perception of the necessity of using Smart Cities technology to improve urban services.......... 99
A.3 Trends in using Smart Cities technology and digital skills 103
A.4 Sense of personal safety 105
A.5 Personal data misuse 107

B Detailed list of requirements for public safety solutions... 110

Members of the IMPETUS consortium 141

Table of Figures

Figure 1. Sample structure by gender 34

Figure 2. Sample structure by age 34

Figure 3. Sources of impact on sensemaking of critical situations 56

Figure 4. Scope, nature and sources of requirements 69

Figure 5. Familiarity with the concept of Smart Cities 98

Figure 6. Necessity to use Smart Cities technology to improve public transportation 99

Figure 7. Necessity to use Smart Cities technology to improve waste disposal 99

Figure 8. Necessity to use Smart Cities technology to improve energy efficiency and management 100

Figure 9. Necessity to use Smart Cities technology to improve smart management of healthcare 100

Figure 10. Necessity of using Smart Cities technology to improve security 100

Figure 11. Necessity to use Smart Cities technology to improve warning systems for high air pollution and other ecological services 101

Figure 12. Trends in using Smart Cities technology 103

Figure 13. Worries about the increasing level of digital skills needed for Smart Cities services 104

Figure 14. General perception of safety 105

Figure 15. Recent change in the level of security 106

Figure 16. Violation of privacy rights and identity thefts („yes" answers) 107

Figure 17. Concern over the misuse of the data collected by the Smart Cities services 109

List of Tables

Table 1: List of abbreviations 10

Table 2: List of definitions 10

Table 3. Integrated IMPETUS solutions, Safe Cities Index. 26

Table 4. Stakeholders of public safety solutions 27

Table 5. Characteristics of two envisaged solutions for Biochemical Risk Detection 44

Table 6. Types of issues arising when new technology is introduced in operational environments 57

Table 7. Summary of operational learning points from recent public safety events 58

Table 8. Format of requirements in Sharepoint List 72

Table 10. Familiarity with the concept of Smart Cities – by gender 98

Table 11. Familiarity with the concept of Smart Cities – by cities (%) 99

Table 12. Perception of necessity of using Smart Cities technology to improve urban services – by cities (%) 101

Table 13. Trends in using Smart Cities technology – by cities (%) 103

Table 14. Worries about the increasing level of digital skills needed for Smart Cities services – by cities (%) 104

Table 15. General perception of safety – by gender 105

Table 16. General perception of safety – by cities (%) 105

Table 17. Recent change in the level of security – by gender 106

Table 18. Recent change in the level of security – by cities 106

Table 19. Violation of privacy rights and identity thefts („yes“ answers) – by cities 107

Table 20. Concern about misuse of personal information (%) 108

Table 21. Concern about misuse of personal information (the averages - (“1” is “Not worried at all”, “5” is “Very worried”) – by cities 108

Table 22 .Concern over the misuse of the data collected by the Smart Cities services – by cities (%)......... 109

Abbreviations and definitions

Table 1: List of abbreviations

Abbreviation	Explanation
CCTV	Closed-circuit television (video surveillance)
DoA	Description of the Action i.e., the part of the Grant Agreement specifying the work to be done in the project

Table 2: List of definitions

Term	Definition
Requirement	"A requirement is a singular documented physical or functional need that a particular design, product or process aims to satisfy"[1]

[1] https://en.wikipedia.org/wiki/Requirement

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

1 About this deliverable

1.1 Intended readership/users

The primary audience of the deliverable is the project consortium.

A secondary target audience consists of stakeholders of public safety solutions for smart cities, including city officials, security and emergency actors, technology providers and civil society.

1.2 Why would I want to read this deliverable?

The central objective of this deliverable is to provide the requirements for the development of the results of project IMPETUS (platform, specific solutions, frameworks).

The requirements are motivated by a background section that contains rich knowledge about public safety operations and technology. This content gives a highly diverse and multidisciplinary set of perspectives on the topic central to the project, i.e. the use of technology to support public safety. Such content therefore serves as a source of information to facilitate learning and collaboration across partners.

For consortium members: The requirements provide a common reference point concerning details of what we will develop together and validate in the two pilot cities according to their specific objectives and needs.

For stakeholders outside the consortium: In addition to the specific needs of the two pilot cities, the requirements also deal with generic challenges or operational needs that can be relevant in many cities. They can therefore be useful to other stakeholders in gaining clarity about their own needs, forming policies and strategies about dealing with public safety in an effective way, and in decision-making about technology adoption.

1.3 Structure

The document is organized into two main parts:

- Part I corresponds to the background information that informs the content of the requirements. This part starts with sections 2 (state of the art) and 3 (perception of stakeholders), which provide the context of public safety solutions in smart cities. Sections 4 to 6 describe the many issues associated with technological solutions for public safety, i.e. relative to technical, operational, and legal and ethical aspects.
- Part II provides the requirements themselves. It starts with a description of their content and development process (section 7), then provides a list of all requirements developed at the time of production of this document (section 8). To further inform the requirements, section 9 provides information on the needs and feasibility of the project's technological solutions, in particular from a technical standpoint (e.g., data needs).

Appendices provide more information on some of the research conducted and further details of all the requirements listed in section 8.

Note that the requirements presented in section 8 and in Appendix B are generated from an online tool (customized SharePoint list) used to register and manage all requirements. That list can continue to evolve and be refined as the project proceeds and deeper understandings are gained. So what is provided here is essentially a "snapshot" of the requirements at the date of production of this document. The snapshot is sufficiently detailed and complete to provide a major milestone in the project, and steer development work. But we also have the flexibility to adapt and refine requirements continuously without the need to issue a new formal deliverable.

1.4 Other deliverables that may be of interest

D1.1 describes the context of the partner cities. It provides richer and more specific content about existing initiatives, security challenges faced and how partner cities envision they could use the types of security technologies considered in the project. D1.1 is for internal consortium use only and is classified as RESTREINT UE/EU RESTRICTED, meaning that strictly defined procedures must be followed to be able to access it. D1.1 is one of the sources used as input to the requirements defined in this deliverable (see section 7.1.2) in the sense that some of the specific requirements are motivated by understandings of context developed in D1.1, but no information from D1.1 is revealed in this deliverable. D1.1 should be considered by all partners as providing an important complement to this deliverable.

This deliverable provides the requirements for the development efforts conducted in all work packages producing software or accompanying frameworks (WPs 2-6). As a result, deliverables produced in these WPs will make reference to the relevant list of requirements and describe how these are addressed. In particular, WPs producing software will make requirements more concrete through specifications.

In addition, requirements aim at being concrete enough to constitute a solid basis for the validation of many of the projects' results. However, the details of this validation is the responsibility of WP7. D7.1 will specify how functionalities and interface characteristics described in the requirements will be evaluated in the project.

PART I. TECHNOLOGICAL SOLUTIONS FOR PUBLIC SAFETY IN SMART CITIES

Part I aims to provide generic information about security in smart cities. Its main objective is to inform requirements, including beyond the specific context of the partner cities to ensure the project's results are applicable and implementable elsewhere.

This first part starts with a state of the art covering the use of technology in smart cities, and more particularly for security purposes. A second section describes the perception of the main categories of stakeholders, i.e. city officials, security actors and the population. These different sections draw on literature, real-world examples and events, and data collection with stakeholders.

Separate sections follow and address different types of issues and challenges associated with the use of technology for public safety. These issues cover the different topics of interest in the project, i.e. technological considerations, but also aspects related to the link between technology and operations and ethics. These sections aim to describe the main questions that are associated with public safety applications, in particular typical challenges with their development, implementation and use. We explore also what public safety issues these technologies appear to solve or improve. Sources of information include return on experience from the implementation of such solutions, associated with real cases and described in the literature (report, academic papers). We want to focus on real applications or advanced experimentations rather than on general fears or promises associated with these technologies.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

2 State of the art: technological capabilities currently implemented in smart cities

The term “smart city” has several definitions depending on the country, legal contexts, type of technologies considered, and so forth. The International Telecommunication Union (ITU) provides the following definition: a smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, the efficiency of urban operation and services, and competitiveness while ensuring that it meets the needs of present and future generations concerning economic, social, and environmental aspects [1]. Therefore, the typical all-connected vision of the smart city is strictly related to the Internet of Things (IoT), which is a combination of embedded technologies such as wired and wireless communications, connected with sensors, actuator devices, and physical objects [2].

A smart city is therefore an urban area in which different technological-based solutions and sensors are networked to collect data and to promote sustainable development. Insights gained from the data are used to enhance the quality of life for citizens by managing assets, resources, and services more efficiently. According to a more structured definition, “*a city can be intended as smart when social, economic and environmental factors are adequately balanced and linked via processes to more efficiently manage key assets, resources, and urban flow for real-time processes*” [1][2]. Smart cities are designed and developed around a framework mainly composed of Information and Communication Technologies (ICT) with Internet of Things (IoT) enabled sensor technology [3]. In this way, a smart city can benefit social and urban interconnectivity through greater citizen interaction and government efficiency. It may therefore be more prepared to face challenges than a traditional city based uniquely on citizen engagement, and not fully interconnected [4].

Several cities throughout the world have embraced the smart city concept and philosophy and have developed or implemented the infrastructure toward a smarter city, or are actively adapting their existing assets and networks [5]. According to Forbes (2019), these include London, New York, Paris, Amsterdam, Reykjavik, Tokyo, Busan, Dubai, Stockholm, and Santander.

This section aims at illustrating the state of development of the smart city concept and giving insights on some specific examples of typical smart city applications. A special focus is given on public safety applications and stakeholders of public safety solutions within a smart city developing framework.

2.1 Typical smart city applications

The concept of the smart city is usually based on a framework, predominantly composed of Information and Communication Technologies (ICT) that are connected to develop, deploy, and promote sustainable development solutions to address present and future urbanization challenges.

Smart city designers make use of modern infrastructures and solutions such as mobile cloud computing, electronic objects, sensors and networks, and machine learning technologies to enable cooperation and interaction among all components of the network architecture [6]. What is typical and usually found in the definition and implementation of a smart city is the application of a wide range of electronic and digital technologies, the use of ICT to outline life and improved working environments, the embedding of ICTs in government systems, and a sort of territorial coverage that brings ICTs and people together. In other words, it is a city whose concept is to monitor and integrate conditions of all its critical infrastructures to better optimize its resources, to plan preventive maintenance activities, and to monitor safety and security aspects while maximizing services to its citizens (Smart Cities Council, 2014). In this way, the utilization of ICT can sustain liveability, workability, security, and sustainability of smart cities since all resources (natural, human, equipment, buildings, and infrastructures) are optimally managed [7].

From a general perspective, the smart city, via an ICT embedded infrastructure, is expected to facilitate addressing many societal challenges and needs, among which: climate change, population growth, economic globalization, demographic, risk, and ecological dependencies, technology development, geopolitical changes, human mobility and migrations, population aging, social conflicts and inequalities, insecurity, and changes in the governmental and institutional sectors [8]. Information and Communication Technologies (ICT) are crucial to make efficient use of infrastructures aimed at allowing sustainable development from

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

an economic, social, and cultural perspective. Besides, ICT plays a key role in involving the citizens at the local administration level by including e-participation intelligence. Finally, ICT is essential to support learning from experience, adaptation, and innovation in order to adapt rapidly and successfully to various changes. What the ICT infrastructure can support is therefore a strong interaction of all dimensions of the smart city starting from digital communication networks, the intelligence integrated into systems, sensors and physical components, and software tools in a comparable nerves-brain-sensorial organ-knowledge mechanism [9].

Different studies proposed a layered vision [10] to better understand the technological complexity and heterogeneity of ICT applications to support smart cities, namely the sensor layer, the integration layer, and the intelligent layer.

2.1.1 The layered vision of Smart Cities

(1) The sensor layer

It is the lowest technology level in the city and comprises sensing devices used to detect and monitor environmental and biological data, including environmental and biometric sensors, online video surveillance, recognition and testing, GPS, water, power, and energy monitoring. The most prevalent technology application in the Sensor layer is GPS, which is mostly used in smart government and smart mobility applications. In smart government, it is most frequently used for smart emergency response systems. GPS can immediately provide important location information during emergency rescue and response operations. Transport administrators and users both require real-time traffic flow monitoring to facilitate vehicle control and provide a more pleasant transport experience.

Wireless sensor networks (WSN) based intelligent transportation systems (ITS) have emerged as a cost-effective technology that bears a pivotal potential to overcome traffic jams and the rising number of accidents. This technology enables traffic safety, traffic congestion control, road state monitoring, vehicular warning services, and parking management [11]. With WSN, different types of motes can be used to sense, process, and transmit data to optimally manage complex situations and enable real-time adaptive traffic control systems. Data of interest include position, traffic condition, local weather, images, acceleration, trajectories, and so on. Some possible sensors include magneto resistive, light, pressure, infrared, video, etc.

(2) The integration layer

The second layer is considered as the backbone of the IoT systems and it allows local storage, data processing, and Internet connectivity that is required at this level to send the collected data to the cloud database. The sensors could generate a huge amount of data per second by making it necessary to pre-process the data locally before sending it to the cloud database. This leads to reducing the volume of unnecessary data sent and stored in the cloud database, with considerable economic savings on data transfer and storage. Microcontrollers help IoT devices store and pre-process collected data before it is synchronized with the cloud database. Microcontrollers possess a processor, a small amount of RAM to hold data, a few kilobytes of EPROM or flash memory to hold embedded software, and solid memory to store data. A related study is presented in [12], where the authors propose the extension of the design of integrated sensory systems based on Arduino, which is widely used for home safety and security systems [13].

(3) The intelligent layer

This layer focuses on the use of cloud computing services, machine learning, and big data analysis technologies. A literature review is proposed in [14] regarding the analytics methods capable of analysing sensor data produced by the smart cities. Several machine learning methods could be utilized to implement the intelligent layer. The Growing Hierarchical Self-Organizing Map (GHSOM) proposed in [15] is a machine learning method that has shown its potential to perform anomaly detection and forecasting on a variety of domains that could characterize smart cities. However, GHSOM can analyse only numerical attributes. This led to enforcing a pre-processing pipeline of the geo-referenced sensor data that could be unsuitable for quick or real-time analyses. Moreover, GHSOM needs to iterate over the dataset several times, which could be infeasible with large real-domain datasets. Spark-GHSOM [16] extends GHSOM to work with mixed attributes (i.e., numerical and categorical) which better describe the real scenario of the data acquired from geo-referenced sensors. Such a peculiarity allows analysing the data produced by the sensors as they are, avoiding the effort and the time consumption for their transformation into numerical values. This aspect could favour the pipeline from the sensor data acquisition to the construction of the predictive models by decreasing the overall necessary time to handle and analyse data. Moreover, this approach is capable of handling big data in a distributed fashion, which enables it to analyse large real-world datasets on a distributed cluster of computational nodes. Therefore, Spark-GHSOM could be utilized to process different domain data (i.e., air pollution, water pollution, traffic level, etc.) leading to preventively identifying a threat from the geo-referenced data via sensor data forecasting. Spark-GHSOM achieved an improvement of up to 79.82% over the considered competitor support vector regression (SVR) developed in Apache Spark [17].

Another interesting task could be considered also in cases when the sensors transmit unlabelled data. In this scenario, the clustering task could be performed to better organize sensor data in subgroups (clusters). To this aim, in DENCAST [18], the authors propose a clustering algorithm that can build a clustering model also for large amounts of data in a distributed fashion. Moreover, DENCAST can exploit annotated data if provided to perform multi-target regression. Multi-target regression could be performed to predict the level of threat regarding different variables such as traffic, air/water pollution, weather conditions, and so on. The results obtained by DENCAST showed an improvement of the predictive performance up to 29.2% when the prediction regards different variables simultaneously [16][18]. The system could be employed with a Model-based BigDataAnalytics-as-a-service (MBDAaaS) approach to handling the huge amount of sensor data that could be generated by the geo-references' sensors in smart cities. Actually, like all methods for the training of predictive models, Spark-GHSOM and DENCAST must undergo an initial adjustment, since the accuracy increases for an increasing number of training examples. João Gama et al. [49] explained further this phenomenon also by illustrating the example of the C4.5 algorithm, which produces a starting predictive model with the first small set of examples by achieving a low accuracy (62%) and it becomes more stable when it observed a greater set of examples. MBDAaaS from sensors data should be performed by considering the starting problem affecting the predictive models described by João Gama et al. [49]. This aspect emphasized the need to switch from a starting state to another when the predictive models become more stable. We can consider three different states: 1) initial state; 2) model adaptation; 3) prediction. The initial state can be overcome by considering a batch learning phase to train a starting weak model to become a more stable one. In the second state, a batch/micro-batch learning approach could be considered to continue the model learning also with small sets of data per time. In the last stage, when the predictive model becomes sufficiently accurate, it can be delivered in production to perform the effective predictions for every single instance of the stream sensor data. Depending on the specific needs, a remote control may be necessary to be able to switch states. To this aim, representational state transfer (REST) services could be helpful to better control the current state of the change detectors and event classifiers at hand. REST is a de-facto standard for a software architecture for interactive applications that typically use multiple Web services [50].

All these layers and components can support the smart city within a common platform, although many applications are still under development and often represent a set of disjointed and limited applications. The actual framework that emerges from the literature is still far from the typical all-connected vision of the "smart city" as conceptualized by the ISO standard 37120:2018. According to the ISO standard 37120:2018, a set of directions of development should be considered when dealing with typical applications of ICT in support of the smart city concept [19]. These directions refer to infrastructures, services, and administrative services required for creating a suitable environment to achieve different characteristics of the smart city.

The main applications of ICT, through which the main objectives of a smart city can be achieved, are:

- smart buildings
- educational, medical, and social care
- smart energy
- smart grid (natural gas, water, electrical energy)
- smart utilities (water distribution, urban waste management)
- strategic urban planning
- smart parking
- integrated supply systems
- smart and integrated transports
- mobile applications for citizens.

As an example, smart buildings can incorporate the advantages of communication and control systems to optimize heating systems, ventilation, and air conditioning.

Similarly, ICT can be successfully applied in terms of applications that allow improving the activity in the educational, medical, and social care domains and ensure access for all citizens to high-quality services.

A smart electrical energy system that interconnects all utilities and end-users with a smart infrastructure can support the optimization of the network operation, compliance with environmental standards, and efficient smart lighting.

Real-time consumption metering of energy, water, and energetic vectors within a smart grid framework, is provided, for example, by wireless smart meters that communicate with an on-line information system.

Smart wastewater systems and real-time solid waste monitoring can be included in intelligent city management of the water distribution systems and wastewater.

The smart parking philosophy may benefit from parking sensors and CCTVs that allow for real-time vehicle monitoring. This is strictly linked with the concept of smart and integrated transports where CCTVs for traffic coupled with smart parking networks are essential for effective traffic monitoring within an optimization concept of all means of transportation while minimizing the impact on the environment. Strategic urban planning based on ICT provides public transportation, as well as housing, electricity, water, and sanitation for a densely settled urban population, while concurrently taking into account the impact of human activities on the environment.

2.1.2 International examples of Smart Cities

Several examples of smart cities exist that effectively benefit from the abovementioned ICT. For instance, New York has developed different ICT applications [20] that are listed below.

- **Smart public transport**: Transit Signal Priority (TSP) is a combination of hardware and software that allows the traffic light to turn green or stay green whenever a city bus approaches the signal. By prioritizing city buses, their average speed could be increased, and it would better stick to timetables. To make the TSP work properly, the Department of Transportation (DOT) studied the traffic patterns at a given intersection. In addition, DOT has installed and operates 750 speed cameras in 750 speed zones in school areas. These cameras use radar and laser technology to measure the speed of the vehicle. If the speed is above 10 miles the image of the vehicle is recorded with the license plate image which is further checked by trained DOT personnel. If the vehicle is found to be exceeding the safe limit, the Liability Notice will be issued to the person in whose name the car is registered. Citibike is another project for smart and sustainable public transport. It comprises 13,000 bicycles at nearly 800 stations. These bikes can be used according to the concept "Unlock, Ride, and Return". First, the bike should be unlocked from one of the stations, then it can be ridden for 30 or 40 minutes depending on the user's pass, after which the bike must be returned to any of the stations.
- **Water management**: A large-scale Automated Meter Reading (AMR) was implemented by the New York Department of Environmental Protection to get a clearer picture of water consumption. Effective methods for using water wisely are "Greywater" and "Rainwater Harvesting". Greywater includes all wastewater apart from that from toilets and can be further used in non-potable activities, i.e., irrigation or flushing into toilets. To provide drinking water to people wandering the streets, several portable water fountains are used as part of the "Water on the Go" program.
- **Waste management**: The government has deployed “Big Brelly”, a smart trash can, throughout NYC. It is a set of garbage cans that contains a wireless sensor used to monitor the level of waste, useful for planning collection trips efficiently. There is also garbage disposal in these garbage cans that runs on solar energy. With the help of the waste comparator, the garbage container can hold up to 500% more waste than a normal garbage can.
- **LinkNYC**: There are over 2200 connections in New York that provide fast, free, public and faster Wi-Fi, free phone calls, device charging, and a tablet for access to city amenities, maps, and 311 apps for government information and non-emergency services. LinkNYC is completely free as it is funded through advertising. Each Link has internal sensors that are used to understand the

environmental impact on structures, and it is robust enough to withstand extreme heat and cold, earthquakes, vandalism, and theft.

- **Smart lighting:** The existing streetlight systems were replaced with an energy-efficient LED which has longer lives. LED lamps allow for better dimming control than standard streetlights. Connected digital LED lighting can be used to create a dense network of sensors and actuators to gather real-time data on traffic, pollution, crime, and more. Many projects in New York are LED lighting retrofits contributing to savings of over $ 800,000 annually and preventing more than 900 metric tons of greenhouse gas emissions.
- **Park management**: With smart parking, mobile charging and additional seating are provided free of charge. Besides, more information is gained on how people use the parking, and through this information, the government can also decide the budget to invest.

In [21], the authors analysed different case studies of smart cities. For instance, Busan is the first smart city in South Korea that exploits the opportunities of the IoT infrastructure. Safety services for children/elderly, drone-based smart marine, smart parking, crosswalk, and energy usage are developed. Moreover, Busan improved the transportation system and e-healthcare services by increasing jobs and business opportunities and improved information accessibility through various devices and communication sources. Chicago, Illinois, in cooperation with IBM, deployed around 300,000 smart IoT devices to reduce energy waste. Moreover, another goal is achieved through an analytics platform on Cisco technology that has helped to minimize crime rates in the city. Also, a predictive model was created for the prediction and prevention of rodent infestations. Analytics is also incorporated to identify buildings that are anticipated to become vacant. Numerous apps have been built using 600 datasets of an open city portal to notify citizens about several unwanted situations expected within a territory. Santander, Spain, is equipped with approximately 20,000 smart IoT devices that perform several measurements such as weather conditions, speed and position of vehicles, traffic intensity, air quality, water networks, and so forth. The acquired sensor data is transmitted to a laboratory to be processed by a central computer for analysis.

In [22] the author shows the case study from the city of Coral Gables, Florida, and how it leverages IoT to improve the quality of life. Coral Gables has implemented a smart city engineering framework that features a wide range of cyber-physical systems (CPS), IoT platforms, and smart connected devices for numerous applications. Specifically, it is based on the transport layer of resilient high-speed communications with fibre optics and wireless infrastructure that covers the city's most critical arteries, facilities, smart neighbourhoods, as well as college campuses and residential areas. The city's IoT systems are based on distributed cloud platforms and data centres where data is aggregated, integrated, analysed, and correlated in a business intelligence and analytics backend with machine vision, artificial intelligence, and machine learning capabilities. Real-time IoT data is viewed and presented to the public and all stakeholders for consumption and collaboration via the Coral Gables Smart City Hub public platform. Coral Gables uses a horizontal integration model that implements a geographic information system (GIS) and data-centred approach for smart city interoperability. A centralized city dashboard gives executives and staff complete and robust visibility into business functions and environmental variables. The project includes key metrics and performance indicators by location, as well as the ability to retrieve real-time GIS-based, location-sensitive information from multiple different sources connected to the data market through a central data bus with inter-cloud replication and management centralized API. Data governance rules and unified access control mechanisms are built into the security, privacy, and compliance model.

2.1.3 Smart Cities in Europe

In Europe, the concept of smart cities has been developed widely across the whole region thanks to many EC-funded projects [23]. Many of these projects have focused on the sustainability of the cities, addressing the energy efficiency of buildings, areas, and districts, both in terms of energy system integration (i.e., photovoltaics and waste heat recovery) and in terms of mobility and transportation (i.e., traffic control systems, bicycle infrastructure, and clean fuelling infrastructure). This focus is asserted also thanks to the Smart Cities Marketplace, an initiative supported by the European Commission [24].

The list of EC-funded projects is not exhaustive: many other projects, in collaboration with private companies, have been completed during the years [25]. As reported by a 2014 study of the European Parliament [26], in 2011 240 of the 468 EU-28 cities (51%) with at least 100,000 inhabitants can be classed as Smart Cities. This number increases to 90% if cities with more than 500,000 inhabitants are considered [24]. Among these projects, a few examples of European Smart City applications can be mentioned:

2.1.3.1 *Copenhagen, Denmark*

The capital and most populous city of Denmark was awarded the world's smartest city in 2014, thanks to its plan for the collection and use of big data ("Copenhagen Connecting") and is the world's 6th smartest city according to the seventh edition of the IESE Cities in Motion Index 2020 [27]. Around 250 companies are currently involved in smart city activities in the city. In 2017 the Copenhagen Solutions Lab has been created in order to manage all the Smart Cities aspects, and in which the Smart City projects are tested and implemented. To improve transparency, the Copenhagen data is available for use by citizens and businesses [28]. The main Copenhagen smart implementation is related to the following intervention areas:

- *Sustainability*: This is one of the focuses of the city. Among all the Goals to be achieved [28], we can cite the data-based energy monitoring and smart building management, in which energy and heat are optimized based on remote reading data; the Street Lab, in which, by using digital technologies, resources and services are optimized; the Greening tool, which is used to calculate a greening factor for a project area/district plan area before, during and after a construction project or a district plan. Moreover, Copenhagen uses noise loggers to listen to the sound of water leaks in pipes, and sensors have been installed in some intersections to create deeper insights into the connection between traffic regulation and air pollution.
- *Smart parking*: The City of Copenhagen is using a combination of historical data and real-time data, algorithms, and machine learning to predict where to find vacant parking spots. The data is retrieved from 30 different sources, which are mostly related to parking and traffic, but the algorithm includes also extraordinary events, such as incidents, excavation work, etc. The precision of the algorithm is around 85% for weekdays and around 80% for weekends (due to fewer data). The parking data is available free of charge for the developers.

2.1.3.2 *London, United Kingdom*

The capital of the United Kingdom is the world's smartest city according to the seventh edition of the IESE Cities in Motion Index 2020 [27]. This position is held since 2017. The city launched the Smarter London Together project, which aims at developing a flexible digital master plan for the implementation of even more smart applications.

All the data retrieved from the city has been directly available to the users since 2004. London focuses on several aspects of the city, transportation, air quality, housing, etc. It is interesting to notice how London provides a dataset that is related to public safety, in which crimes are recorded (divided per borough), as well as information about fires and incidents. London also provides an official roadmap of the upcoming (and completed) targets. By consulting the roadmap [29] it is possible to learn which smart city applications have been implemented and which remain work in progress.

It is worth to cite two further city case studies [30], Antwerp (Netherlands) and Barcelona (Spain), which, in partnership with the mobile operator Orange, retrieve data from the mobile devices connected to the network to know the density of population in an area in real-time. This is done independently from the fact that the mobile phone is owned by a resident or a visitor. In the city of Barcelona, the tourist attraction the Sagrada Familia is monitored, both in terms of the number of visitors throughout the day and their arrival route. Antwerp goes a step further deploying a crowd management solution for local events, such as the hosting of the Tour de France. The data is retrieved from the connection of phones to masts across all the available mobile networks, collecting both the position and timestamp of a device. All the information is available by using a unique, anonymous ID. Also, Vienna (AT), Aachen (DE), Milan (IT), Sestao (ES), Tampere (FI) and Bratislava (SK) have participated at some European initiative, like the *European cities serving as Green Urban Gate towards Leadership in sustainable Energy* project (*EU-GUGLE* - *http://eu-gugle.eu*), and have committed to renovating a total of 226,000 m² of living space during the project to increase the share of renewable energy sources by 25% by 2018.

2.1.4 Example outside Europe: Boston, United States

Boston is known as a dangerous place for bicyclists and pedestrians. The road structure, like that of many European cities, was laid out for horses and carts and now is populated by a large number of cars. Additionally, Boston drivers have been ranked #1 worst in the United States by Allstate insurance, and they are known for parking habits that obstruct the roadways and viewpoints.

In 2016 the Boston Mayor and other leaders undertook a program known as Vision Zero, inspired by a similar 1997 Swedish program, to reduce fatalities and serious injuries. The program consisted of infrastructure changes, information campaigns, and technology-driven safety modifications.

Infrastructure changes were made, such as building more bicycle lanes (though few included physical separation from traffic). In addition, the program used ICT to encourage citizen engagement and awareness to enhance the benefit of the program. In this case the ICT was an enabler, not the direct producer of the desired benefit.

One of Vison Zero’s ICT projects used software based on a thin client Graphical User Interface (GUI) interfaced to an Environmental Systems Research Institute (ESRI) map of the Boston metropolitan area, together with a driver’s smartphone application built by Cambridge Mobile Telematics. This software was well implemented, intuitive, and widely accepted. The map-based approach used a GUI on which users recognized familiar streets and intersections. Bostonians could see hazard reports geolocated on the maps and add their own inputs. A telephone hotline was also available. Over a three-year period, while this software was being used, fatalities were cut in half and, according to Allstate insurance, Boston became only the second most dangerous city in the US.

There was another, less-successful app tried for Vision Zero, that attempted to track aberrant driver (car or bicycle) behaviour using a smartphone application (https://www.cmtelematics.com/news/boston-app-grades-driving/). The application graded driver behaviour using raw data generated from the phone sensors together with machine learning and statistics. The hope was that the grade would motivate the driver to improve his behaviour.

During the initial use of the app, there were some benefits observed. Among users there were decreases in risky behaviours: a 47% decrease in distraction, 35% reduced speeding, and 63% fewer sharp turns. But driver acceptance of the application fell below what was needed for the app to have significant impact. Privacy fears and apathy may have deterred acceptance by individual drivers, and Boston organizations were less eager to promote the app because it was a distraction from other public initiatives such as the ALS Ice Bucket Challenge, and the push for more people to use public transportation.

2.2 Specific examples of public safety applications

While people move to cities for a variety of reasons, we all have one expectation in common: that we will be safe. We want our growing cities to provide us with better access, greater energy efficiency, and more convenience than ever before. At the same time, we need our cities to be able to ensure the safety of their citizens. In many ways, the smart city movement is providing the infrastructure necessary to increase public safety. What cities are discovering is that the infrastructure that is built to help make them more efficient can also be used to safeguard their citizens. What is becoming clear is that public safety must be a pillar of any smart city strategy from the very beginning. Ultimately, even in the most technologically advanced city in the world, if citizens do not feel safe, businesses cannot succeed, and the city will not thrive. The ability to collect and understand ever-increasing amounts of data will improve how cities provide services and protect their citizens in the future. Ultimately, cities, in collaboration with the private sector and technology providers, will be creating ecosystems of systems. This unification will have an even greater impact on public safety. In the future, when an event occurs, harnessing a city’s system of systems will exponentially improve situational awareness. It will also have a similar impact on the time required to collect the appropriate information and perform an investigation.

2.2.1 Safe city concept and its features

A "Safe City" is one in which data and technology can be harnessed to keep residents safe. Possibly the most comprehensive definition of a safe city is provided by the Economist's “Safe Cities Index” [31]. The index can assess cities across the world based on forty-nine indicators (in 2017) and fifty-seven distinct factors (in

2019) - covering digital security, healthcare security, infrastructure security, and personal security - to identify the safest cities and those with the highest number of security vulnerabilities. The Safe Cities Index (SCI) is an interesting benchmarking tool since it not only measures the crime on the streets but has a broad range of security inputs and results, which also may give input to the validation plan of IMPETUS (WP7). There are four distinct areas that the SCI focuses on, that include digital, infrastructure, health, and personal security. In the latest index [32] (2019, its 3rd edition), a new measure was introduced; that of 'urban resilience', an indication of how quickly a city could get back on its feet after a shock. Rather than trying to create a fifth distinct pillar of security, the index now measures new areas within the other four pillars of particular relevance to resilience such as disaster-risk informed development policies.

Digital security assesses the ability of urban citizens to freely use the internet and other digital channels without fear of privacy violations or identity theft. On the input side, cities are scored on their awareness of digital threats, the level of technology employed, and the existence of dedicated cybersecurity teams. On the output side, the index measures the frequency of identity theft and the estimated number of computers infected with a virus.

Health security measures how cities maintain the natural environment as well as the level and quality of care available. On the input side, cities are scored based on their environmental policies, access to and quality of healthcare services. Output indicators include air and water quality, life expectancy as well as infant mortality among other sub-indicators. A new sub-indicator focusing on the number of chemical, biological, and radiological attacks on a city was also included to incorporate the impact of terrorism on urban health systems.

Infrastructure security considers the built physical environment, such as city infrastructure and its vulnerability to disasters and terrorist attacks. On the input side, the index considers sub-indicators such as the quality of infrastructure as well as the enforcement of transport safety, while on the output side the number of vehicular accidents and pedestrian deaths are included, as well as the number of terrorist attacks on facilities and infrastructure.

Personal security considers how at-risk citizens are from crime, violence, and other man-made threats. Input indicators in this domain take into account policies and decisions such as the level of police engagement, the use of data-driven crime prevention, and the overall political stability of the country where each city is located. On the output side, the index considers the prevalence of petty and violent crime, safety perceptions, as well as new sub-indicators assessing the threat of civil unrest, military conflict, and terrorism.

Put simplistically, outputs measure how safe a city currently is, while the inputs indicate which cities are doing the right things to enhance safety. The scores in the four index pillars, though, turn out to be closely correlated. Correlation does not prove causation, and the relationship between different kinds of security go both ways. Nevertheless, part of the connection is a frequent reliance of other pillars on digital security. Technology plays an obvious role in digital security, but new developments, for example, in data mining and artificial intelligence (AI), are opening some intriguing new possibilities in other pillars. The application of AI to data to improve and enhance digital, health, infrastructure, and personal security. The message from the data is not that digital security, or indeed technology, is the silver bullet for urban safety. Instead, the index results indicate that a safe city is one where efforts made by citizens, stakeholder groups, and authorities in a wide range of fields to reduce and protect against various kinds of risks, mutually re-enforce each other to create a generally secure environment.

2.2.2 Innovative solutions for safety in cities

Examples of low-cost steps and innovative solutions and example applications that can improve different elements of city safety.

2.2.2.1 Personal safety

Personal safety can be enhanced through the use of several smart city technologies, in some cases by adding to or co-opting the technologies' primary function, for instance:

- Video surveillance cameras, such as CCTV and traffic license readers can help detect, deter, and anticipate crime (see examples below);

- Smart street lighting [33] can detect activity and turn on lights to deter crime or warn potential victims, and also provide an infrastructure to support sensor deployment and digital signage;
- A smart city's WiFi infrastructure [34] can support emergency call boxes and public address systems, enhancing public safety;
- A smart city's communication infrastructure [35] can use social media to (1) communicate information to the public that promotes safety during an emergency; and (2) harvest information from the public to guide safer response to situations.

As an example, in Nairobi, Kenya, a new strategic communication network has been put in place that links 1,800 surveillance cameras with more than 190 police bureaus and 7,600 police officers. The infrastructure is a response to recent terrorist strikes that have undermined travel to the country and is intended to support public security and help tackle civil unrest. It technically relies on a wireless eLTE solution that links the National Police Service command centres with a high-definition camera network in Nairobi downtown, cameras at city checkpoints, and any number of wireless devices used by officers in the field. Besides, an intelligent video analysis platform has been implemented to meet a variety of services, including video browsing, real-time surveillance, and data sharing.

Another example of safety and security included in a smart city concept is that of Mexico City. An integrated urban security solution was proposed, based on a large-scale video protection approach. Almost 15,000 CCTV cameras were installed in the city and an integrated system that relies on panic buttons and loudspeakers is used for earthquake warnings and public order communications. The solution has been intended to reinforce the police presence on the streets, according to also a reorganization of police districts. The Mexico City police has been equipped with trucks packed with communication systems, drones, and high-tech apparatus. Additionally, a digital filtration of incoming calls to avoid false alarms has been implemented and officers can analyse and include video sequences in an emergency response operation.

Similarly, a partnership is supporting the SafeCity project in Nice, France. The city is becoming one of the most important pilots of safety through full-scale tests. The project intends to offer and implement a complete security system including video protection for road safety, school security, and patrols connection. Such a security system is based on a combination of different technologies: cameras mounted on the city's streets are supported by mobile cameras that can be used for specific purposes and multi-lens HD cameras. The infrastructure includes also geo-localization of municipal police patrols, building alarms connected to a control centre, and an automated system to control retractable anti-intrusion bollards. In Nice, a real-time video protection system has been mounted also in public transportations, complementing the already existing public transport CCTV system. The new concept makes use of a Wi-Fi link to provide real-time reporting of accidents, violations, and crime instances.

Predictive policing, including a mathematical and analytical technique to identify criminal activities, are deployed by the New York police according to a criminal group database. The police can rapidly retrieve detailed information and a machine learning algorithm, known as Patternizr, links potential criminal suspects and unsolved cases. Similar systems are implemented in the United Kingdom and Russia. Cameras around the city (more than 120,000) can identify faces and are interfaced with complex infrastructure to support different policy duties, among which recognizing traffic and red-lights violations. This implementation falls within a wider New York police surveillance plan that was further developed and implemented following the September 11 terrorist attacks. It consists of active surveillance of a wide range of public activity and collection of data used by prevention departments to arrange police operations, counter-terrorism actions, and to face domestic violence. The infrastructure is based on a combined operation of CCTV cameras, sensors, machine learning platforms, data analytics systems, and mobile apps.

2.2.2.2 *Infrastructure security*

Infrastructure capabilities were firstly adopted in Nanjing, China, in 2013 during the Asian Youth Games. For the event, an integrated infrastructure managed data of key areas, including all stadiums and surroundings. The city has taken the application further including by connecting drone-mounted cameras. To date, the infrastructure has also integrated private communications, video surveillance, dispatch functions for private and public facilities, and services related to emergency response.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

The next-generation 911 (NG911) initiative in the United States and Canada is focused on the update of existing 911 service infrastructures to enhance the public emergency response via promising technologies. The NG911 operates over internet-based networks that can digitally transmit a vast array of data. Smartphones enable citizens to share detailed real-time data that police, and dispatchers can review and send directly to responding officers. One of the world's first examples of this was adopted in Groningen, Netherlands, where the police introduced the mobile app ComProNet (community protection network). Within the NG911 concept, the Vancouver Police department is actively using predictive models based on big data and analytics to detect city areas where break-ins are anticipated and to best allocate police officers. The NG911 also includes the scope of dealing with operational Artificial Intelligence (AI) to prioritize calls to the police and to consolidate responses to similar incidents.

Around 2016, the MOLIT (Ministry of Land, Infrastructure, and Transportation), in Korea, started building and implementing a spatial data platform as a location-based big data analysis system. Through spatial information analysis, this platform is designed to support the policy-making process including safety. For instance, a pedestrian safety map against crime has been successfully implemented in some Korean cities, as well as crime prevention environmental design (CPTED) through intelligent CCTVs and fences. Similarly, to other cities, in Busan, more than 5,000 CCTVs of the urban network are connected to an intelligent information system that detects early signs of crime. The target is to make use of a system able to also include integrally this aspect among other smart city challenges, namely energy management, air pollution, and noise management. CPTED concept is also at the basis of the crime prevention technique implemented in the Pyeongataek-Godeok New City project where natural monitoring and access control are expected to reduce the conditions of crime. According to this implementation, existing infrastructures are used to investigate vulnerable areas through spatial analysis and Tracking Management Systems. Furthermore, CCTV installation locations are selected according to the outcomes of the analysis. Safety zones are codified and identified and people crossing are provided with notification services. At the same time, citizens can shake the smartphones alerting the police about adverse safety scenarios.

In the Seoul neighbouring city of Anyang, the Smart City Centre is operative. It is mainly devoted to traffic monitoring, but it can be adapted to track different scenarios at the same time. For instance, in the presence of emergencies, CCTVs start to monitor and configure the emergency spot also with a GIS platform.

In Pittsburgh [36], 200 intersections have been equipped with specific technology to improve the traffic flow: sensors determine traffic volume and optimize stop-and-go times. Research have shown that vehicles in East Liberty intersections spend 40 percent less time idling, resulting in a 21 percent emissions reduction. Denver [37], in collaboration with Ericsson, is implementing an ATMS (advanced traffic management system), which gives the ability to aggregate and analyse real-time data from monitoring devices, such as traffic sensors and cameras, controllable traffic lights, etc. This solution can be shared with adjacent municipalities to improve the traffic data.

What emerges from the literature analysis of existing infrastructures converted/used for public safety applications in the smart city concept is that there is a need for city planners, energy sector decision-makers, governments, and law enforcement agencies to continuously expand and innovate public safety initiatives. Areas of intervention include advanced data collection, optimized techniques, and disaster and crime prevention, in which ICT and IoT technology may give a relevant contribution.

Generally, the literature underlines the primary ways these technologies have impacted or will impact, the public safety concept. Firstly, ICT and IoT can have a major impact on smart devices that improve policing and law enforcement. As an example, the deployment of body sensors and cameras supports real-time notifications during escalating scenarios, giving evidence to criminal cases, and increasing police accountability. Or even, IoT applications can be associated with the collection of detailed accounts of criminal activity (tracking services for location, movement, activity). Secondly, gun violence and offense can eventually be decreased through the use of IoT gunshot detection that may play a key role in impacting law enforcement's ability to manage public safety during shooting incidents. For example, noise and frequency detectors are used to triangulate the location of active shooter incidents. As a third consideration, emergency healthcare can have advantages from the use of a connected medical wristband that recognizes typical symptoms and automatically calls for help, or again wearable sensors and smart contact lenses can give emergency alerts on health diseases.

Finally, prevention of environmental pollution and issues related to safety and security during natural disasters are focus area for ICT and IoT integration in existing infrastructures. IoT can help to combat flooding and adverse events in urban areas via live updates based on sensor networks and supporting the implementation of effective evacuation planning. Similar solutions are to be implemented in monitoring hazardous areas and sites prone to the pollution that can detect failures and integrity issues, both during regular and anomalous safety- and security-related frameworks.

It is possible to use very cheap devices (including open-source hardware such as Arduino) to track all sorts of relevant environmental factors, from energy to temperature, water, air quality, etc.

2.2.2.3 Health security

Here we will focus on the rapid identification of chemical and biological agents. The Tokyo subway sarin attack was an act of domestic terrorism perpetrated on 20 March 1995, in Tokyo, Japan, by members of the cult movement Aum Shinrikyo. In five coordinated attacks, the perpetrators released sarin on three lines of the Tokyo Metro (then part of the Tokyo subway) during rush hour, killing 12 people, severely injuring 50, and causing temporary vision problems for nearly 1,000 others. The attack was directed against trains passing through Kasumigaseki and Nagatachō, where the Diet (Japanese parliament) is headquartered in Tokyo.

The Organisation for the Prohibition of Chemical Weapons (OPCW) lists several toxic chemicals defined as "*any chemical which through its chemical action on life processes can cause death, temporary incapacitation or permanent harm to humans or animals*" [38]. There are several types of agents such as choking (irritate the nose, throat, and especially the lungs), blister (affecting the eyes, respiratory tract, and skin, first as an irritant and then as a cell poison), blood (inhibit the ability of cells to use oxygen, effectively causing the body to suffocate), nerve (lock an enzyme called Acetylcholinesterase (AChE) in the nervous system. This causes the accumulation of a neurotransmitter between nerve cells or across synapses leading to hyper-stimulation of muscles, glands, and other nerves), and riot control agents (intended to temporarily incapacitate a person by causing irritation to the eyes, mouth, throat, lungs, and skin).

A wide variety of detection equipment is available commercially. Tests, detectors, and monitors are based on the following technologies and techniques: Ion Mobility Spectrometry (IS), Electrochemical sensors, flame photometry, Thermoelectric Conductivity, Infrared Spectroscopy, Photoacoustic IR Spectroscopy, Photo Ionization Detectors (PIDs), Surface Acoustic Wave (SAW), Color-Change Chemistry, Raman Spectroscopy, Mass Spectrometry, Gas Chromatography, Fourier Transform Infrared (FTIR) Spectrometry. Current R&D in chemical agent detector technology is focused on increasing the speed and sensitivity of the instruments, while at the same time bringing down their size and cost.

Bioterrorism is terrorism involving the intentional release or dissemination of biological agents. These agents are bacteria, viruses, insects, fungi, or toxins, and may be in a naturally occurring or a human-modified form, in much the same way in biological warfare. Biological agents can be spread through the air, water, or in food. Biological agents are attractive to terrorists because they are extremely difficult to detect and do not cause illness for several hours to several days. The 2001 anthrax attacks, also known as Amerithrax (a portmanteau of "America" and "anthrax") occurred in the United States (Washington D.C., West Palm Beach - Florida, New York City) over several weeks beginning on September 18, 2001, one week after the September 11 terrorist attacks. Letters containing anthrax spores were mailed to several news media offices and Democratic Senators Tom Daschle and Patrick Leahy, killing five people, and infecting 17 others.

Because biological agents do not immediately produce effects, the first indication of an attack with a biological agent may be the recognition of an unusual distribution or number of cases of the disease, long after the initial aerosol or solution has been dispersed or degraded. The detection of biological agents involves: (1) a probe, and (2) a transducer. Probe technology deals with how the assay or detection device recognizes the particular target microbe. Transducer technology deals with how the assay or detection device communicates the activity of the probe to the observer. Together, probe and transduction systems determine the specificity, sensitivity, and time required to make an identification. Probe technologies include those based on nucleic acids, antibody/ antigen binding, and ligand/receptor interactions. Transducer technologies include electrochemical, piezoelectric, colorimetric, and optical systems. There are some detection devices in which there is no clear division of probe and transducer. Methods based on physical properties and separation are good examples: mass spectrometry and gas or liquid chromatography. To the interested reader, we refer to the following book [39]: Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response.

2.2.2.4 Digital security

Smart cities focus on solving challenges due to population rise in urban areas, such as physical security, residual management, and transportation systems [40]. Smart cities integrate cyber-physical systems, self-organizing devices, fog computing, wireless sensors, IoT devices. The growth of the world-wide urban population and the increase of this demographic make the smart cities' cybersecurity very important. All the smart city components are exposed to cyber-attacks. In the sequel, we present existing approaches in the cybersecurity literature aiming at securing smart cities from cyber-attacks.

Ivanov et al. [41] propose a method that includes a calculation of security indicators, risk assessment, and countermeasures based on attack graphs. Thus, it allows the consideration of the dynamics of changes in the components of the smart infrastructure. They use Python to develop a system that assesses the security of smart cities. The tool contains four modules: (1) data processing module; (2) risk assessment module; (3) countermeasure selection module; and (4) visualization module. The data processing module converts the input data and the data from the countermeasure selection module into classes that implement operations on the attack graph. This module parses the input data and builds the attack graph. The attack graph is then used by other components to evaluate the security, develop countermeasures, and build a visual model. The risk assessment module calculates the main risk indicators. It makes a comparative assessment of the current state and the preceded state by removing one of the existing vulnerabilities. In the countermeasure selection module, the tool performs an iterative search for the optimal countermeasures. The application of the countermeasures consists of the elimination of the most critical vulnerabilities. The visualization module sends data about the attack graph to the attack graph visualization service.

Botello et al. [42] propose BlockSIEM, a blockchain-based and distributed Security Information and Event Management (SIEM) solution to protect smart city services. BlockSIEM gathers security events from different IoT service providers, storing them in a distributed ledger of a blockchain [43] that keeps them utterly secure against any unexpected modification. This approach uses both internal and external threat intelligence to detect and prevent cyber-attacks against the smart city services and intelligent devices, promptly alerting about an in-progress attack. A smart city is composed of IoT devices. An IoT sentinel is in charge of protecting a set of IoT devices in its proximity against cyber-attacks. Whenever an intrusion attempt arises, the IoT sentinel generates security events and builds a transaction request sent to the set of SIEMs enabled as miners; they have mining and security functions. Those SIEMs mine the transaction and add it to the blockchain in the form of blocks. Concerning the security functions, a SIEM enabled as a miner analyzes all of the security events in the blockchain's distributed ledger to detect or prevent cyber-attacks. BlockSIEM is based on a permissioned blockchain, Ethereum, that only allows known nodes to be part of the network.

Falco et al. [44] developed a tool to evaluate the cyber risks to critical infrastructures in smart cities. They propose the automation of the attack tree generation process using AI planning techniques. They develop a master attack methodology used by classical planners to generate automated attack trees by combining many respected authorities' attack frameworks. The phasing sequence of the attack leverages Lockheed Martin's cyber kill chain [45]. The surface area of where the attack could occur references the Open Web Application Security Project's (OWASP) attack surface areas. The actions required to accomplish the given phase of the attack is represented by both MITRE's Common Attack Pattern Enumeration and Classifications (CAPEC) [46] and MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework [47]. Finally, the tools used to execute the actions are represented by both Kali Linux tools and known exploit tactics by MITRE's ATT&CK Matrix. Leveraging these frameworks, the authors compile a master ontology database that accounts for virtually all known attack vectors across all system types.

Garcia-Font et al. [48] propose a non-intrusive architecture designed together with Barcelona's city to bring the WSNs control back to the system administration and monitor the providers. Furthermore, the system allows detecting incidents due to known and unknown attacks, preventing contagion, and stopping their effects. The proposed solution is based on an enhanced SIEM within the city council facilities to use recollection, storage, processing, and big data services offered by the smart city. The key aspect of their proposed architecture is built around two detection engines: (1) an SVM-based detection engine (which permits to detect attacks that have not yet been disclosed or for which a signature would be too complex to be implemented) and (2) a rule-based detection engine (with a higher degree of detection accuracy). Administrators can easily implement rules to detect misuses and correlate the alerts triggered by the SVM-based detection engine to reduce false alarms.

From the works surveyed in the previous section, we observe that the work of Ivanov et al. already uses an attack-graph-based method to minimize the security risk due to intruder penetration in a network of a smart infrastructure from any of the system nodes. The method consists of removing the most critical vulnerabilities on the nodes. Also, the work of Falco et al. proposes a master ontology database that can be used with classical planners, while augmenting semantics for attack tree generation purposes. Inspired by the previous approaches, we sketch in the sequel a cyber threat response optimization approach for smart cities based on the combination of SIEMs, attack graphs, ontologies, and attack simulation using cost-sensitive metrics.

2.2.2.5 Applications under development, developed and implemented

The four pillars of the Safe Cities Index Framework also provide a link to the integrated IMPETUS solutions (Table 1).

Table 3. Integrated IMPETUS solutions, Safe Cities Index.

IMPETUS Tool	Safe Cities Index
Social media detection (SMD) tool	Digital security
Weapon & face detection (WFD) tool	Personal safety
Biochemical risk detection (BRD) tool	Health security
Breach and attack simulation (BAS) tool	Digital security
Cyber threat intelligence (CTI) tool	Digital security
Physical threat intelligence (PTI) tool	Infrastructure
Human-computer interaction (HCI) tool	Personal safety
Physical threat response optimization (PTRO) tool	Infrastructure
Cyber threat response optimization (CTRO) tool	Digital security

2.3 Stakeholders of public safety solutions

The purpose of a public safety strategy, and related solutions, is to develop, implement, and monitor results-focused, evidence-based strategic initiatives to ensure that a vision of a safe and secure city is achieved. Many actors are involved in emergency management and are interested in public safety solutions, given that the context of public safety is complex and public safety solutions have implications on numerous aspects of the smart city concept. A successful model for public safety within a smart city framework should necessarily deal with the mobilization of all city departments, bringing together a diverse set of stakeholders, and consulting with as many members of the community as possible. This inclusive approach is crucial for always finding innovative solutions to complex public safety challenges and the different actors cooperate to forge public-private partnerships that combat criminal activity. An improved and better use of data and technological capabilities is essential to increase transparency, to break down informational barriers between law enforcement and citizens, and to enhance the collaboration of communities to identify needs and establish best practices to preserve public safety.

In this framework, the stakeholders to consider relative to public safety solutions can be categorized within specific but ideally coordinated groups, summarized in the following table:

Table 4. Stakeholders of public safety solutions

Stakeholder	Role	Examples
Regulators	Regulate the implementation of security technology in public places	Policy makers at the city, national and European level
Decision-makers	Decide on investment in security technology solutions	• city managers, smart city managers • regional & national security agency managers • critical infrastructure managers
Security actors	Use the technologies in security operations	• police and other security agencies, contractors • city, regional, national level • operators and managers
Emergency actors	Interact with primary users in managing security events	• emergency agencies' actors and managers • critical infrastructure operators
Population	Residents of the smart cities, impacted by the use of the technology	citizens (including citizen groups)

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

3 Perception by stakeholders

This section presents results from investigations of the perception of public safety technologies from the main types of stakeholders. Data was collected using different methods for the different stakeholders.

3.1 Cities: officials and managers

Officials and managers, in their decision-making role, are among stakeholders of public safety solutions in a smart city concept. According to [1], the emergency management policy process deals with some stages in which the safety and security policy formulation and adoption are essential for a successful strategy. In this strategy, city officials and managers can be in charge of discussing and driving the development and implementation of public safety and smart city solutions. In a smart city framework, they have a decisional role and may be involved in decisions about the level of attention and resources allocated to local emergency management.

Officials and managers can support mitigation and preparedness practices and have a great deal of influence on local emergency management policies and practices. It should be noted that the emergency management process is fundamentally a local issue for which a smart city integrated public safety system is activated. However, in addition to local governments, regional and national level managers have a number of important emergency management functions. This organizational structure is aimed at protecting citizens and their possessions through the active involvement of public organizations, police forces, and citizens themselves. An active and proactive approach to collecting and monitoring information for crime prevention is also expected.

Officials and managers group of stakeholders include:

- city managers and smart city managers,
- local, regional, and national security agency managers,
- critical infrastructure managers.

The general opinions about Smart City technologies of city officials have been drafted according to the findings of the focus group analysis in the partner cities.

Different spheres have been investigated including:

- general opinions about ethical issues in Smart City technologies and sense of personal security
- personal experiences of participants
- smart city areas that generate ethical issues
- privacy issues
- tracking pedestrian, consumers, and vehicles
- tracking selected populations
- data use issues
- overseeing the ethical implications of Smart City technologies.

3.1.1 General conclusions of the focus group analysis

In general, according to participants, using anonymously collected data for the purpose of better management is not perceived as a highly significant issue by city officials. Responders are, on the contrary, concerned about the ethical problems that could arise from lacking the minimum information necessary for the involved person to make a rational and motivated choice; even if, in specific countries like Italy, the legislation in terms of correct use of data is stringent.

Some concerns are connected to online payments and transactions and a potential threat in integrating different data from many sources in profiling, which can lead to some unfair conclusions. The problem arises mainly in situations where personal data used for some specific purpose (GPS, location data, …) is shared with third parties (e.g., with commercial interests).

Video surveillance and CCTV-based information are not seen as a big issue, but related data can be misused. As an example, mobile applications for car parking can be used as a marketing tool showing habits, everyday routines, etc.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

According to the opinions of respondents, maintaining privacy while browsing the Internet is difficult, but the main concern is that AI processing techniques and algorithms are used in combination with personal information to link some persons to distant or inadequate persons, web pages, organizations, etc.

When speaking about respondents' line of work, in general there seem to be ethical issues, but still there is a problem with mixture of different data and how to prioritize. One of the solutions for keeping data safe is protection by both internal and external organizations.

Smart mobility is seen as the area with the highest possibility of initiating ethical issues, but the most sensitive issue regarding data privacy is tracking of spatial mobility – benefits for collecting such information are easy to see, but such data is personal, almost an on-time diary of someone's life. Tracking of pedestrians, consumers and vehicles has almost the same issues.

Tracking of selected populations such as prisoners, people on probation and other specific populations that can be a threat to the community or themselves is considered acceptable for the majority of the focus group participants and they agree that this is an efficient way of controlling and monitoring such subpopulations. Some respondents noticed that this can also have some unwanted consequences such as racial profiling in crime prediction systems.

Finally, participants think that, besides collecting consent and providing information to citizens about which personal data is being collected, a code of conduct and a committee that publishes general guidelines to help the cities manage ethical issues should be established. Of special concern is the use of data gathered about vulnerable populations such as elderly, who are not well informed about the Smart City technologies. The participation of civil society, local action groups and other citizens' initiatives is welcomed.

To conclude, the following quotes from participants are relevant. It can be noted that such perspectives are controversial and at the heart of trade-offs of interest in the project; they might also conflict with the spirit of European regulations and recommendations:

- *«Any system that can increase the security of places and people [...] is always ethically acceptable»*
- *«[...] the safety of the population is a priority over the ethics of the individual».*

3.1.2 General opinions about ethical issues in Smart City technologies and sense of personal security

Generally, the participants do not think that there is a significant ethical problem with the use of the collected data in their countries. Personally, some of them are concerned about the security of online payment transactions, as well as potential unethical use of the data that can be collected from various sources and integrated in order to «profile» someone or just to misuse data in some other way to harm the person. It looks like respondents from city officials are, at least slightly, less confident than respondents from emergency services that there are sufficient and trustworthy ways to store such data.

3.1.3 Personal experiences

In their line of work, the participants do not see many ethical issues, aside from:

(1) combining data from different sources beyond what the citizen has consented to, and
(2) giving different priorities depending on who the citizen is.

Respondents said that they use sharing tools such as clouds, Google Drive, Dropbox etc. only for non-sensitive data or data that cannot harm others outside of their work. However, there is a need for protection of materials/data collected from various sources and it should be done both by internal and external regulatory organizations.

When comparing the answers from the city officials and the other respondents that work in emergency services there seem to be little to no differences between their answers, i.e., the issues stressed by both groups are similar.

- **Smart city areas that generate ethical issues:** Smart mobility is seen as the area with the highest possibility of ethical issues. Even when used for valuable and reasonable purposes, such information can still be misused. However, respondents did not show strong concern that administration and public bodies will not have some legal restrictions, strict control and/or solutions that can keep such data safe at the strongest level.

- **Privacy issues:** Tracking of spatial mobility is seen as the most sensitive issue regarding the data privacy because use of such data can possibly impact other areas that include privacy of identity, transactions, leisure time movements etc. However, all this data is already utilized in city traffic management, public transport systems and other. There is a general feeling that all data gathered in fact cannot be seen as independent from each other, although this feeling is more apparent in respondents from emergency services.
- **Tracking pedestrians, consumers, and vehicles:** Even though the participants think that tracking pedestrians, consumers and vehicles is a legitimate part of Smart City technologies, they also see possible challenges (e.g., surveillance misuse by authorities or private companies, specific targeting of some populations, etc.). Use of mobility data *per se* is not considered a big ethical issue if it is used for improvement of security and traffic. It should be noted that respondents from city officials described and marked this area even less questionable and misleading compared with answers from the of emergency sector group.
- **Tracking selected populations:** Control/monitoring of prisoners, people on probation and other specific populations that can be threats to the community or themselves is acceptable for the majority of the respondents. Even though the participants think that tracking selected populations is generally acceptable, they do see various ethical issues that can arise in the process, most related to using such information more frequently than needed. For instance, some of them think that only publicly available data should be used, that such tracking can be given overstated attention (and, conversely, paying too little attention to other law-enforcing methods) and that such methods could lead to racial profiling (in case of crime prediction systems), etc. This seems to be more questionable for city officials compared with the opinion of representatives of emergency services.
- **Issues related to data utilisation:** The participants think that Smart City data should be used only for its stated purpose, i.e., that any form of re-packaging the data is not permissible, even when completely anonymous. All use of data by commercial or political organizations can only be done with permission and consent of the persons involved, but there will still be a risk of misuse.
- **Overseeing the ethical implications of Smart City technologies:** The participants think that a code of conduct and a committee responsible for publishing general guidelines to assist the cities in managing ethical issues should be established. Regulation of the use of data gathered about vulnerable populations such as elderly, who are not well informed about the Smart Cities technologies, is of particular importance. The participation of civil society is welcomed.

3.2 Emergency and security organisations: managers and personnel

This section summarizes perceptions of emergency and security personnel regarding public safety technologies, i.e., those whose work will be impacted by the implementation of IMPETUS results. The analyses are based on information from the IMPETUS focus groups described in the last section, and from the published reports of two comprehensive surveys:

- A 2020 Canadian survey of perceptions of successes and failures in technology implementation from Canadian police leaders [2]
- A 2018 – 2021 US National Institute of Standards and Technology (NIST) survey of over 7,000 first responders entitled Voices of First Responders – Identifying Public Safety Communication Problems [3 - 9]. This survey used interviews and large-scale questionnaires among first responders to to identify:
    - communication and technology needs,
    - beliefs and perceptions about their current technology,
    - what they would like their technology to do, and
    - why they do and do not use technology.

Results about emergency and security personnel perceptions are summarized according to three areas:

- Ethics and privacy
- Technology implementation
- Other operational considerations.

3.2.1 Ethics and Privacy

Ethics and privacy were the primary focus areas of the IMPETUS focus groups, and perceptions concerning these issues surfaced in both the Canadian and NIST surveys.

In the Canadian survey, respondents called for the need to test technology against community expectations to determine whether the technology being acquired poses any ethical dilemmas for the police service or its members. They stated that the technology acquisition process needs to include an examination of community expectations and determine whether the technology's capability would be considered appropriate by the community. The respondents proposed that the police service must be willing to discuss their ability to risk-manage the integrity of their information holdings and how they are using advanced analytics/artificial intelligence to carry out their mission in an ethical way.

The IMPETUS focus group participants generally did not see a significant ethical problem with the use of collected data in their countries. Focus group participants from emergency services were overall confident that collected data will be used in trustworthy ways.

In the NIST survey, emergency responders were generally sensitive to their role in ensuring proper use of collected data. Their concern with situations that cause vulnerabilities, such as open cell phone communications or monitored radio channels demonstrated an alertness to proper data use.

In the IMPETUS focus groups, participants, especially those from emergency services, saw a major privacy issue with data being aggregated from the many data collection sources being used today. While individual data collections may seem unobtrusive, analysis that combine them with other data may lead to profiling, discrimination, and political manipulation to influence or interfere with citizen behaviour. Focus group participants made it clear that smart city data should only be used for its intended purpose, and not repackaged, even if completely anonymous.

In the NIST survey, many responses expressed concern about how easy it is to add and withdraw material from the cloud. Respondents understand that the large volume of data that can be collected in this manner creates opportunities for misuse. However, the survey respondents pointed out how convenient it is to have data readily available for patients, so they can get on with the work of actually helping the patient without being delayed by data collection or complications in report writing.

Focus group participants were particularly concerned that location and movement data collected in transportation systems, cell phone location, etc. could be unethically used to monitor and profile personal movement.

In the NIST survey, while responders were fully aware of privacy issues associated with location and movement data, they also saw this data as very helpful to them for performing their jobs. For example, if a policeman's movement can be tracked while chasing a suspect, he or she can concentrate more fully on the chase rather than being distracted by calling in locations and changes in direction during the pursuit.

Generally, IMPETUS focus group participants believed it acceptable to track people who might be threats to the community. Some were concerned that the misuse of this tracking data could lead to less effective and potentially biased policing. Emergency service participants believed the benefits of using this data outweigh the potential for misuse.

NIST survey respondents made it clear that tracking potential threats is key to their work, and that law enforcement organizations create and use special identification numbers to track potential threats.

NIST respondents were also concerned about the public's use of scanners to listen to first responder communication. This permits the public to pick up sensitive information about incidents if first responders are not vigilant.

They were also concerned that the availability of smartphones and smartphone apps creates vulnerabilities to leaking sensitive data. The capabilities of personal smart phones and apps can make them more convenient to use than official equipment. For example, taking a picture and sending it is easier using a smart phone than trying to use an officially provided digital camera and a flip-phone. This can result in trading off operational efficiency and data security.

Similarly to city officials and managers, participants in the IMPETUS focus groups from emergency organizations thought use of data and technologies should be regulated in smart cities through codes of conduct and guidelines.

NIST respondents did not express the need for additional oversight of the ethics of smart city technologies, beyond current practices to ensure ethical behaviour in general.

3.2.2 Technology Implementation

The Canadian Study surveyed police leaders, seeking their perceptions of what worked and did not work in their implementation of public safety technologies. The focus of the study on leaders resulted in the identification of critical high-level organizational priorities required for successful implementation:

- Strategic Alignment – the implementation of new technology needs to be guided by a command-level IT strategy that aligns operational needs and acquisition programs with organizational goals, mission, and overall strategy
- Managing Expectations – leaders must ensure that the multiple stakeholders in a technology project have shared expectations concerning the implementation, use, and efficacy of new technologies
- Defining Success – there needs to be a clearly understood and articulated link between the technical solution and the specific problem it is expected to solve, and criteria for success need to be defined prior to the start of implementation
- Acknowledging Technology Debt – acquisition of new technology is frequently constrained by the need to continue to use and invest in legacy infrastructure, and the IT strategy needs to realistically reflect this situation
- Customization and Configuration – surveyed police leaders experienced long delays when technology solutions, often intended to be shared across several organizations, did not fit within their local environments. Technology implementation plans need to realistically assess and account for local requirements
- Information Security Leadership – the complexity and importance of the cyber environment requires knowledgeable and skilled cyber security practitioners who can advise executive management, and ideally creation of a Chief Information Security Officer (CISO) position at the command level.

The responses to the NIST survey were analysed in the study reports and a set of technology implementation guidelines were developed, to remedy issues raised by survey participants:

- First consider improving current technology - improve the functionality of what first responders currently have - make technology more affordable and more reliable. For example, improve radios with better coverage, durability, clarity, better microphones, and cords. The first responders donot necessarily want new technology; improvement of current technology may be more important
- Reduce unintended consequences – do not allow technology to interfere with the primary job of the responder, causing distraction, loss of situational awareness, cognitive overload, or over-reliance on the technology
- Recognize ‘one size does not fit all’ –there are similarities across first responder disciplines and standardization is important for consistency, compatibility and quality, but technology must accommodate the wide variety of public safety needs – across disciplines, personnel, departments, districts, and contexts of use. All are different, and technology must be easily adapted and configured
- Minimize ‘technology for technology’s sake’ – develop technology with and for first responders, driven by their user characteristics, needs, requirement, and contexts of use
- Design to affordability – develop technology at prices that departments can afford
- Require usable technology – develop solutions that are simple, easy to use, light, fast, and not disruptive. Technology should make it easy for the user to do the right thing, hard to do the wrong thing, and be to easy to recover when the wrong thing happens.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

3.2.3 Other Operational Considerations

NIST survey respondents commented on the challenges associated with coordinating the multiple sources of information now available to emergency and security personnel. While old style radios enforced a one-speaker-at-a-time protocol, cell communications can be more chaotic.

New technology can also put additional stress on an emergency responder. Having to deal with password resets, disappearing digital documents, and additional technology to operate and maintain can add workload that can interfere with the primary mission.

Dispatchers in emergency organizations now have access to multiple sources of information in addition to phones. While this can provide a more complete picture, it can also be overwhelming. Also, information can produce additional stress on a dispatcher when, for example, murder or suicide is streamed over the internet.

Internet connectivity with the public provides a rich source of information, however it can be error prone. Emergency responders report many incidences of inaccurate characterizations of events and wrong addresses communicated by the general public.

They also were concerned about verification and admissibility issues associated with the use of information collected from the growing number of private surveillance systems not subject to public control.

Finally, NIST survey participants pointed out that drones are highly cost effective compared to the previous alternative for many situations – helicopters.

3.3 Population: citizens and citizen organisations

3.3.1 Research conducted

A public opinion survey on use of smart technologies in detecting and reacting on security threats in public spaces was conducted during April 2021 in five European cities – Bucharest (Romania), Madrid (Spain), Oslo (Norway), Padua (Italy) and Zagreb (Croatia). The survey was conducted by using the method of computer-assisted telephone interviewing (CATI). The interviews were carried out by telephone aided by the pre-coded responses in a questionnaire displayed on the computer screen, thus minimizing the possibility of errors during the data entering process. The sample in each of the cities was constructed by using various methods of random sampling. Namely, the households were selected by using random digital dialing, while the respondents within the households were selected randomly as well (last birthday method, etc.), thus ensuring that the key demographic characteristics of the population appear with a similar frequency in the sample. The fieldwork in each of the cities was executed by the local contracting public opinion agencies. The sample size in each city amounted to around 500 citizens of 18 years of age and older (Bucharest – 508, Madrid – 502, Oslo – 501, Padua – 500, Zagreb – 507). Such sample size guarantees the maximum sampling error of +/- 4.3% (proportion testing with population parameter of 50%) in each of the cities with 95% confidence intervals. The master questionnaire written in English was translated into local languages by the contracting agencies. Before the start of each interview, a verbal informed consent was obtained.

The data depicted in Figure 1 show that about 53.5% of the participants were female and 46.5% male. As for the age structure, the most of survey participants belong to the 31-45 yrs. age groups – 28.7% and over 60 yrs. age group – 28.4% of them. The average age over the entire sample was about 49.4 yrs., with similar average ages across the cities (from 47.2 in Oslo to 52.1% in Zagreb)

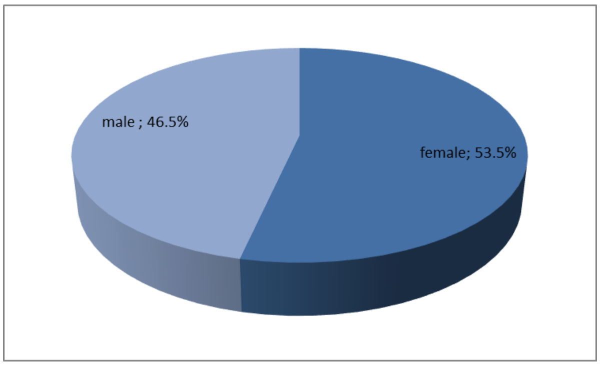

Figure 1. Sample structure by gender

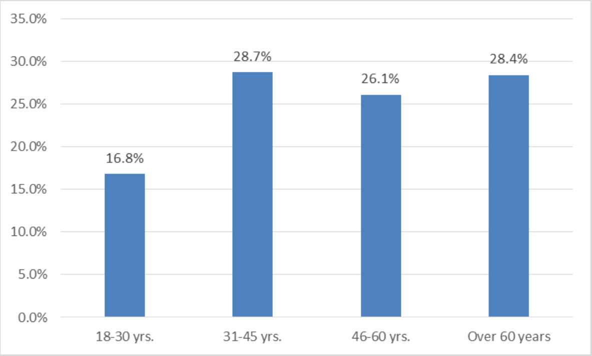

Figure 2. Sample structure by age

This section only provides the summary findings in each of the participating cities. Full results for all the cities combined are shown and explained in Appendix A. Given that only age and gender were collected during the interviews as sociodemographic data, only the potential differences with regards to those two variables were statistically tested. Second, the differences between the cities were delineated in tables, wherein statistical differences were tested using various statistical models (depending on the nature of the variables). As a rule, the technical details pertaining to the statistical testing are omitted from the text.

The main objectives of the research were to probe into the citizens' opinions about various Smart Cities technologies, their possible misuses and other potential ethical issues related to them. In the study, among other things, an attempt was made to determine:

- familiarity with the concept of Smart Cities.
- perception of the necessity to employ Smart Cities digital technologies in order to improve city management and the general urban life.
- perception of the usage of Smart Cities technologies in one's own city.
- perception of the digital skills level needed for successful use of the Smart Cities technology.
- perception of general level of safety in one's own city.
- perception of the change in the level of security.
- negative experiences regarding digital technologies (identity thefts, violation of privacy rights, etc.)
- level of worry in relation to the possible misuses of personal data.

3.3.2 Summary of results

Familiarity with the Smart Cities concept – The largest share of the respondents (43.2%) have heard about the concept of Smart Cities, but they are not familiar with the details. Men and younger citizens are more familiar with the concept. Citizens of Padua expressed the highest, and citizens of Oslo and Zagreb the lowest level of familiarity.

Perception of the importance of the Smart Cities technologies – The participants generally agree that there is a need for incorporating Smart Cities technologies into urban management. Women are more likely to think that some of the uses of Smart Cities technologies are important in comparison to men. Padua citizens are the least likely to think that Smart Cities technology is needed in most of the application areas. Bucharest citizens expressed the highest level of need for such technologies. Oslo and Madrid citizens expressed average level of need for such technologies.

Trends in Smart Cities technology application – The largest share of the participants – 49.4% of them – think that the use of Smart Cities technology in city management in the last five years has slightly improved. The survey participants from Bucharest and Zagreb are more often of an opinion that the situation in their city regarding the use of Smart Cities technologies has not improved. The participants from Padua largely think that the situation has been improving, but only slightly. The participants from Madrid, and especially Oslo, more often think that the situation has improved significantly.

Smart Cities technology and digital skills – Almost 60% of the participants are not worried or not worried at all about their personal digital skills needed for Smart Cities services. Female respondents are more often worried about this issue than male, while older citizens are also more worried. Citizens of Oslo, and

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

especially Padua, are not worried because of the increasing level of needed digital skills, citizens of Madrid and Zagreb are the most likely to be worried, while Bucharest citizens are placed in the middle.

Sense of personal safety – Citizens generally feel safe living in their city. Males feel statistically significantly more safe than females, but the differences are not very pronounced. Bucharest citizens feeling the least secure on average. About 60% of the participants estimate that the security level has not changed significantly. Most citizens of Bucharest think that the (in)security level present in their city exists for some time. Padua citizens compare their current security situation much more favourably in comparision to the earlier situation.

Experience of personal data misuse – The violation most often experienced personally is use of data for unnecessary or unwanted purposes. Males more often reported the cases of violation of privacy rights and use of data for unnecessary or unwanted purposes. All cases of violations are more often reported by younger citizens, probably due to their more frequent use of various digital services. Zagreb citizens rarely reported such problems, especially when it comes to identity theft and withdrawal of money. The situation in Padua is similar, with the marked exemption of use of the personal data for unnecessary or unwanted purposes (marketing campaign, telephone directory, contact-lists of some companies, etc.). The situations in Bucharest, Oslo and Madrid are very comparable, but the same exemption applies – Madrid citizens are also very sensitive about the above mentioned use of personal data.

Concerns about personal data misuse – The participants are most concerned for the security of your passwords on the internet. On the other hand, the least concern was expressed for surveillance camera footage. Padua citizens are least concerned about any misuses of their personal information. Madrid citizens are the ones who are most often concerned, except in case of surveillance camera footage, where Bucharest citizens are more concerned. Zagreb citizens are also generally not very worried about the listed misuses, while Oslo and Bucharest are somewhat worried.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

4 Technical issues

In this section, we explore the technical challenges to the development and implementation of public safety technological solutions in smart cities. Issues might include interoperability, data access, cyber security, platform architecture (complexity), infrastructure dependability, technological changes, etc.

4.1 Security and safety solutions

In this section we discuss solutions used in smart cities that are key to successful development and implementation of public safety applications. We discuss solutions in the following categories:

- Cyber security
- Communications infrastructure
- Verification and surveillance
- Biochemical Risk Detection

4.1.1 Cyber Security

In order to increase smart city safety and security and make smart cities less prone to cyber-attacks, multiple roles including stakeholders, governments and cyber security specialists should be involved, as well as enhanced security and safety solutions should be integrated within smart cities. There are two main steps that should be completed for accomplishing this goal, including:

1. **Defining and formalizing the detailed cyber security strategy for diminishing challenges related to the everlasting convergence, interoperability and interconnectedness of the city systems and processes.** As the first step, detailed impact assessment of the smart cities' data, systems and assets should be conducted with the aim of highlighting the potential risks related to technology processes and policies. Attaining the integrated view of risks and interdependencies of the critical assets can assist cities in developing a thorough cyber security strategy. Afterwards, defined steps should be formalized, and required roles and responsibilities should be assigned to the corresponding smart city critical components. On top of that, the establishment of ecosystems for repelling cyber-attacks requires not only cooperation between different entities, but also with other cities, academia, corporations, and state agencies [1]. Furthermore, governments must ensure that policies, legislations, and technology are matured and aligned for sustaining right levels of protection, privacy, transparency, and utility. In order to deal with the problem of skills gap, governments should also employ non-traditional methods, such as crowdsourcing and offering rewards for solving known cyber security issues, as well as establishing strategic cooperation and contacts with service providers [2].
2. **Development and implementation of security solutions consisting of the following features:**
    a. **Data encryption.** Smart cities often utilize sensitive data such as PII. Establishing two-factor authentication can assist in mitigating issue of the potential breaches of such critical data.
    b. **Security monitoring and analysis.** A security monitoring platform captures data regarding the general state of the system, including endpoint devices and connectivity traffic. Moreover, it analyses the data in order to detect potential cyber security threats. Based on the findings, an array of actions, such as device quarantining can then be enforced [3].
    c. **Firmware integrity and secure boot.** Security boot, empowered by cryptographic code signing techniques, can be used to ensure that only the code created by trusted party is executed. As a result, hackers are thwarted from replacing firmware with malware.
    d. **Multi-environment support.** Multi-environment support, i.e., support of on-premises, IaaS, SaaS and hybrid cloud environments ensures that all devices in the smart city are connected.
    e. **Mutual authentication.** Mutual authentication allows for secure authentication of devices to the network prior to transferring data. That way, it is ensured that the data is coming from the genuine source.

f. **Security lifecycle management.** Through lifecycle management feature, service providers can control security aspects of the operating IoT devices in the smart cities. Furthermore, secure device decommissioning prevents ditched devices from being repurposed and abused without authorization [4].

g. **Human machine teaming.** This includes objectively measuring and assessing the human operator state (neuro-physiological, behavioural, performance). The analysis could provide adaptive task and function allocation for workload and decision-making balance between the human operator and a security system component. By considering the human operator as a functional requirement, human-in-the-loop solutions are ensured.

h. **Communications infrastructure.** An Information and Communication Technology (ICT) infrastructure is at the core of smart city operations, and a key component of smart city safety. ICT supports the prediction and detection of danger, situation assessment and analysis, coordination of response, and prioritization of recovery operations.

i. **Verification and surveillance.** These are technologies that enable verification of authorized personnel and support surveillance to assess dangerous situations, and to identify dangerous people.

S1 – Lightweight encryption.

Lightweight encryption algorithms can be implemented in the smaller size smart devices that have restricted computational capabilities and limited memory and power resources, that cannot run traditional cryptographic algorithms. Thus, lightweight solutions can contribute to both reducing memory and power consumption and providing essential security in such devices. Efficiency of the lightweight cryptographic solutions is usually measured based on the performance of different factors, such a key size, block size, number of rounds and structures. Currently, there are four main groups of lightweight cryptographic solutions which can provide both authentication and non-repudiation that can be utilized for IoT devices, including Lightweight Block Cipher (LWBC), Lightweight Stream Ciphers (LWSC), Lightweight Hash Functions (LWHF) and Elliptic Curve Cryptography (ECC), [5] [6]. Lightweight block ciphers are established around substitution-permutation network (SPN) and Feistel structures, where Feistel structures allow for a minimal overhead in encryption and decryption, hence reducing the memory usage in devices. One such lightweight encryption algorithm using block size of 64-bit, key size of 128-bit and nine rounds has proved to be highly secure, while at the same size being energy and memory efficient [7]. Another possible lightweight solution comes in the shape of lightweight hash functions, which transforms a arbitrary-length message into a fixed-length message digest, which can be then used on both low and high-end CPUs for ensuring data integrity. When it comes to asymmetric ciphers, ECC is the most suitable for smaller IoT devices because it uses smaller key size than RSA, while providing the same level of security. However, according to the findings of Danda et al. [8], there is still room for improvement for all four groups of solutions. Moreover, according to the authors, future design of LWBC should be focused on further reducing key size, block size and number of rounds, whereas for LWFH, message and output size should be decreased. On the other side, asymmetric lightweight solutions should be focused on designing better optimized prime fields and group arithmetic in order to speed up execution times.

Class: Data Encryption

S2 – Human behaviour analytics.

Models and algorithms to decode neural, physiological, and behavioural signals show a high degree of promise for application in human machine teaming situations. Investigations of neural-physiological activity related to naturalistic perception, action, and cognition, along with analyses with computational models and machine learning tools can be used to develop interfaces and sensors for human operator interactions with machines. For instance, sensors can be used by machines to integrate neural activity patterns and behavioural observations, in order to infer the human’s intentions and cognitive states, such as mental workload. Although current approaches rely on data-driven decoding of neural-physiological signals, the robustness of brain machine interfaces could be improved by theory-driven models that incorporate an understanding of the neural representations that support high-level cognition (e.g., memory, decision-making, situational awareness etc.).

Class: Human machine teaming

Existing tools (excerpt): Human Interaction Tool

4.1.2 Communications infrastructure

The overall ICT infrastructure of a smart city consists of four layers: terminal sensor layer, communication network layer, platform service layer and city application layer. The combination of communication network with basic technologies, such as cloud computing and AI, is the foundation for many smart city technologies.

CI1 - Radio Frequency Identification (RFID).

Duru and Karas [9], described RFID as a technology that uses the radio frequency to communicate with identifiable objects or people in the smart campus. The authors defined RFID system to consist of a reader, tag, and host computing, and contain electronically stored information that can be read by the RFID reader, thus allowing for automatic real-time monitoring without the actual need for a human presence.

Class: Communication infrastructure

Existing tools: passive, semi-active, and active tags

CI2 - Near Field Communication (NFC).

Near-field communication (NFC) is a type of radio-frequency technology that allows electronics devices—such as computers, mobile phones, tags, and others—to exchange information wirelessly across a small distance. This technology can be used to securely verify identity documentation, such as ID cards or passports [10].

Class: Communication infrastructure

Existing tools: tag reader/writer, peer-to-peer communicators, card emulation

CI3 - WIFI.

WIFI is an IEEE 802.11 standard whose devices can be deployed all over the smart campus to support a huge number of WiFi connections. Smart cities are finding it cost-effective to provide free internet access to users via WiFi, due to its high performance, low-cost and simple technical implementation. Using these WIF services, citizens can instantly seek emergency assistance and provide local situation assessments [11].

Class: Communication infrastructure

Existing tools: routers, repeaters, receivers

CI4 - ZigBee.

ZigBee is based on the IEEE 802.15.4 standard. ZigBee is used to create personal area networks with applications and devices that require a long battery life, lower data rate and secured networking. So, it is often used in monitoring and control applications where data reliability, power-efficiency, and affordability are crucial. Compared with other personal area networks, ZigBee type represents a cheap and simple solution [12] (other options exist, such as Z-Wave).

Class: Communication infrastructure

Existing tools: hubs, smart switches and other devices

CI5 - LTE-TETRA.

TETRA networks are predominantly used for voice, but they also support status messaging, Short Data Services (SDS) or text messaging and multi-slot packet data (MSPD) which provides speeds similar to

General Packet Radio Service (GPRS). TETRA Enhanced Data Services (TEDS) provides speeds equivalent to cellular Enhanced Data Rates for GSM Evolution (EDGE) technology and can handle video if the network is not too congested. Modern IP-based TETRA networks can also support Supervisory Control and Data Acquisition (SCADA), smart grid and telemetry applications. Since its development in the 1990s, TETRA has become the predominant public communications standard for public safety professionals in Europe. As of 2017, there were a total of 27 Public Protection and Disaster Relief (PPDR) national networks in Europe.

It is clear that public safety networks will eventually migrate to some form of broadband solution based on cellular 4G LTE (Long Term Evolution) technology. However, this realisation comes with the recognition that cellular technology, limited as it is to one-to-one person calling, is not currently capable of providing all the key mission critical features that public safety communications users simply cannot do without. Public safety users can send texts, emails, photos, easily access the Internet and watch videos on high-definition screens. Naturally, they would like to be able to do the same on their work communications devices. Due to spectrum scarcity and cost, nationwide private LTE networks for emergency services are unlikely to appear in Europe [13].

Emergency-services agencies in the United Kingdom (UK) are expected to stop using TETRA in 2024 or 2025, when the transition to an LTE push-to-talk solution on the Emergency Services Network (ESN) is scheduled for completion. The ESN will use hardened Samsung LTE device [14].

Class: Communication infrastructure

Existing tools: transmitters, radios

CI6 - 5G.

The evolution to faster 5G networks will improve smart city applications needing high bandwidth and low latency in mobile networks, while enabling the connection of massive small, low-cost sensors, which will provide basic guarantee for data-driven decision-making and governance on a large scale. Transmission through 5G networks will provide better access to the massive data generated by smart cities, unleashing the potential of improved analysis using next-generation information technologies, including AI and cloud computing [15]. In addition, 5G will improve nationwide mission critical or public safety network communications used by emergency services: fire, police and health.

Class: Communication infrastructure

Existing tools: transmitters, radios

4.1.3 Verification and surveillance

These are technologies that enable verification of authorized personnel and support surveillance to assess situations dangers, and to identify dangerous people.

VS1 - Biometrics.

Biometrics is an automatic recognition of a person by using several metrics related to unique human characteristics. They are of two types: behavioural and biological or physiological characteristics. These two types are obtained by applying proper sensors and the typical features are used to obtain a biometric template in the authentication process [16]. Automatic facial recognition from CCTV, news or social media, and from checkpoints is also considered biometrics.

4.1.4 Biochemical Risk Detection

Air pollution is a growing concern because of its impact on health. Air quality assessment mainly relies on static monitoring stations. Europe counts about 1500 air quality monitoring stations. These stations allowed to monitor 5 chemical pollutants and particles matter to provide a real time index of air quality. The main compounds measured are the carbon monoxide (CO), carbon dioxide (CO2), particulate matter smaller than 10 microns (PM10), or particulate matter smaller than 2.5 microns (PM2.5); and some environment elements, including ozone (O3), which is produced by the combination of nitrogen oxides (NOx), Oxygen (O2), Volatile Organic Compounds (VOC), and sunlight [17].

Integration of these data in smart cities development starts to be described. However, biological monitoring of the air is poorly investigated and no integration in smart cities was realised up to now.

Some countries have a monitoring system for allergy-causing agents such as pollens and moulds, but the network is less performing than for chemical pollutants and the data is not easily usable for integration into smart cities.

Concerning the surveillance system of biological harmful agents, for natural transmission or intentional transmission, the only description provides from the BioWatch Program [18]. The other programs to countermeasure against biological agents are focused on the preparedness of the health system. For the JO 2020, which has been postponed due to the SARS-CoV-2 epidemic, the Japan has purchased a smallpox vaccine, and accelerate the research of new drug therapy, SAKIGAKE program [19].

Main characteristics

The BioWatch program is a surveillance system that was created in order to detect the planned discharge of aerosol type biological harmful agents after the anthrax terroristic attack in 2001. This program is deployed in 30 big cities in the United States.

Low information is available on this program except that it was based on 3 parts:

- sampling
- analysis
- and response.

The sampling is realised on the pre-existing air quality monitoring stations. Samples are concentrated on filters and are then analysed by molecular biology in specialized laboratory. The entire pathogen list is not available but principal terrorist agents are researched (anthrax, plague, tularaemia, and smallpox).

The force of this program is the involvement of a large network of stakeholders (public health, emergency management, law enforcement, laboratory, scientific, and environmental health organizations) to prepare a coordinated response to a bioterrorism attack.

Consequently, among the challenges for public security in smart cities can be highlighted in terms of a warning system to detect an act of bioterrorism as early as possible. Bioterrorism is defined as the release or dissemination of biological agents (bacteria, fungi, toxins, or viruses) that can cause illness or death in living organism (human, animals or plants). It exists a large variety of agents that could cause damage in the nature. Moreover, the biological agent may also be altered by bioengineering to increase its resistance to the antibiotics, its viability or to mislead detection methods. The bioterrorism agents may be dispersed in water, in soil, in food or in the air.

On a lot of points, a bioterrorist attack could be assimilated with the propagation of an infectious disease. Currently, the initial detection of bioterrorism attack occurs with the diagnose of the initial patients contaminated by the health care system [20]. This suggests that their number and/or the nature of the disease is surprising enough to be visible. This detection is related to the appearance of the onset symptoms and in case of contagious agent, this delay could lead to the spread in the population of the disease. The response provided must be designed from the detection of the attack to the dissemination of countermeasures.

It must mobilise:

- the authorities in order to maintain the functioning of the institutions
- training of health workers in the early detection of non-conventional diseases and enabling the adaptation of health care systems
- training of first responders
- developing environmental monitoring systems to detect the presence of agents at an early stage

The last point and the integration of an alert system in a smart city could constitute a first step in the risk management with the aim to give a concerted and adapted response.

4.1.5 Gaps and challenges

In this section we provide a list of gaps and challenges. Challenges can belong, but are not restricted to, interoperability, data access, cyber security, platform architecture (complexity), infrastructure dependability, technological changes.

G1 - Gaps on IoT design. IoT is just recently but slowly being designed considering security as principal requirement [21]. In most of the cases IoT system has no defense-in-depth strategy, such as a secure boot process isolation of a Trusted Computing Base just to name one [22]. In addition, basic good practices like limitation of the number of open ports and authentication are normally not considered or are very weakly implemented. In general, the concept of security-by-design or privacy-by-design is not taken into account by most of the IoT manufacturers. In many cases information is exchanged with a third-party without control, credentials are stored as plain text and cannot be modified (hard coded default password). Moreover, a number of IoT systems are implemented in a way to use diverse protocols and technologies that often end up creating complex and conflicting configurations. Another issue is that certain smart devices have obsolete or low-quality hardware or operating systems that do not support advanced security approaches [23].

Smart city components involved: This gap is specific for IoT devices that are largely used in the context of smart city. It impacts all the IoT devices and planning to use them in any smart city context.

Gap classification: interoperability, platform architecture (complexity), infrastructure dependability, technological changes

G2 - Gaps on IoT authorization, authentication and confidentiality. IoT systems rarely adopt advanced authentication and authorization architectures between devices. In addition, some critical tasks like firmware update can be in most of the cases executed without a signature check allowing tampering and usurpation. Similarly, in many situations, software updates are possible without authorization and file trust verification. One of the critical phases of an IoT device is the boot phase where authorization and authentication can help in hardening the device against critical threats. In many situations secure boot is not implemented. IoT is also typically exposed to risks associated to weak password policies or default passwords left unchanged. In order to protect information from being passively attacked or exposed to the attackers, confidentiality of has to be ensured [24]. Ensuring information confidentiality between different nodes calls for encryption, which is often not properly implemented.

Smart city components involved: This gap is specific for IoT devices that are largely used in the context of smart city. It impacts all the IoT devices and planning to use them in any smart city context.

Gap classification: data access, cyber security

G3 - Gaps on Human Machine Teaming. Interactions with technologically sophisticated artificial intelligence (AI) agents are now commonplace. We increasingly rely on intelligent systems to extend our human capabilities, from chatbots that provide technical support to virtual assistants like Siri and Alexa. However, today's intelligent machines are essentially tools, not teammates. They require the undivided attention of a human user and lack the communicative or cognitive capabilities needed to interact as trusted teammates. To become true teammates, the intelligent machines will need to be flexible and adaptive to the states of the human teammate, as well the environment. They will need to intelligently anticipate their human teammate’s capabilities, intentions, and generalize specific learning experiences to entirely new situations. There are challenges [25] to (a) better understand human cognitive capabilities in the context of complex and dynamic situations; (b) to understand what humans must know and learn about machines and their physical and internal structure in order to effectively and efficiently interact with them, including what is required in human machine teaming to establish and maintain trust; (c) to improve intelligent machine capabilities in order to enable effective human machine teams, and (d) to understand and realize the internal representations and processing of a machine required for reasoning about human teammates.

Smart city components involved: This gap is specific for City Command & Control Centres. It impacts all the IMPETUS tools to use them in any smart city context.

Gap classification: human machine teaming

G4 - Communications Interoperability

An Information and Communication Technology (ICT) infrastructure is at the core of smart city operations, and a key component of smart city safety. ICT supports the prediction and detection of danger, situation assessment and analysis, coordination of response, and prioritization of recovery operations. In addition to its support of city safety, ICT vulnerabilities themselves become an added safety issue.

Smart city technology is employed in many sectors of city operation, such as energy, buildings, transportation, utilities, surveillance, health care, and education. Since all these sectors are concerned with and are participants in public safety, it is important that they can effectively communicate, to achieve a common understanding of situations, and to effectively collaborate.

Effective communication among smart city sectors is multi-layer challenge, involving coordination among organizations, operations, and communications technologies. Because individual smart city sectors often procure and develop smart city technology separately, interoperability can be a problem. Even if sectors decide to collaborate in developing standards, vendor lock-in to proprietary solutions can interfere with or prevent interoperability [y].

Smart city components involved: this primarily affects the ability of different smart city sectors (energy, police, fire) to collaborate. As sectors develop their own communications systems, interoperability is usually guaranteed within a sector. Communications standards and a good city-wide communications architecture are required and affect all smart city components.

Gap classification: interoperability

G5 - Unbiased and Effective Automatic Surveillance

Automatic facial recognition in CCT footage, check points, and in online news and social media can be an effective way to identify terrorists and other dangerous people, and to deny unauthorized access. Modern facial recognition software uses deep artificial neural network technology, which relies on millions of example training images to calibrate parameters that enable distinguishing different faces [26].

The technology has the potential to be extremely helpful to authorities faced with identifying bad actors in the massive volume of digital imagery data being collected in smart cities. Recent advances in artificial neural networks have made the technology better and better, however it has an important limitation, with two major consequences.

The limitation is that facial recognition software cannot generalize beyond the training images it has been calibrated on. The software 'sees' the minute details of faces and uses these details in a very literal way. The two major consequences of this limitation are (1) the software can make mistakes that would be immediately obvious to a human observer; and (2) it can exhibit biases and inaccuracies in recognizing the faces of minorities, since minorities are underrepresented in the training images [27].

There are two approaches being used to reduce the gap between actual and desired performance. One approach is to improve the technology so that it is less biased. Researchers are actively pursuing this improvement.

Another approach is to create procedures that use the results of facial recognition software as only an alert, with the understanding that additional means will be required to verify identity. While this sounds straightforward, police departments have found that even the presence of a non-verified alert can lead to undesirable bias [28].

Smart city components involved: CCTV analysis systems; identification checkpoints

Gap classification: infrastructure dependability

G6 - Interoperability of data exchange standards

There are several data exchange standards for public safety management applications, for example, Global Justice XML Data Model (GJXDM), Emergency Data Exchange Language (EDXL), National Information Exchange Model (NIEM), Emergency Communications (EMTEL), etc. All these standards provide a suite of protocols for structuring information for analysis and public alters. Such data exchange standards are necessary to support effectiveness, efficiency, and transparency objectives for public safety communication [29]. Hence, it is important to felicitate and increase the implementation of these standards into the commercial public safety technologies.

However, there are still challenges of the suitability of these data exchange standards for demanding real-time public safety applications. The particular challenges could be about the application development community agreeing on the most appropriate data exchange standard for a data type format. In addition, the public safety application development companies need to encourage adapting open-data exchange standards in their respective products. The standards such as FIWARE open source platform for Smart Cities [30] and oneM2M global IoT platform standard [31] are interesting candidate in addressing interoperability related technical issues to build smart city systems. Examples of case study of the cities using FIWARE and oneM2M based deployments can be found in Bordeaux [32] and Busan [33].

G7 - APIs for real-time sharing and collaborative sharing

The open APIs and standards are equally essential to achieve objectives of future smart cities and to enable utilization of the collected data across platforms in real-time using technologies such as AI or ML. One such example of API is an open framework for the exchange of contextual data for smart services, named NGSI-LD [34] and developed by ETSI. In the future, technological solutions may adopt these open APIs, however, integrating them into the existing solutions and extracting context from already collected historical data (if un-structured and non-standardized) pose technical challenges to the developers.

G8 - Cyber security assurance

Numerous companies are providing public safety and security technology solutions in smart cities. As safety and security technology solutions handle sensitive public data and integrated it into the national critical infrastructure, a security breach in their product or company assets could expose a pathway to compromise the smart city itself. However, evaluation of cyber security processes within these companies and in their product raises technical challenges for smart city owners. These challenges vary from the availability of resources to perform a security assessment of safety and security solutions before the actual deployment. The emerging issues such as the compromise of companies providing facial recognition technology [35] and security products or applications such as traffic light systems [36] or surveillance camera system [37] indicate a lack of secure product development and product lifecycle processes. Hence, smart city owners may require a technical standard or framework for cyber security assurance from technological solutions. An example of such cyber security framework could be an inspiration from NESAS (Network Equipment Security Assurance Scheme) technical specifications [38] proposed to define and introduce a baseline security level in 5G systems. In addition, Zero Trust Architecture [39], proposed by the NIST may assist in providing zero trust principles to public safety and security solutions used in smart city domain.

G9- Gaps on Biochemical Risk Detection

The initial detection of a bioterrorist attack is currently based on the vigilance of health personnel who detect the abnormal appearance of the onset symptoms. The approach developed in the IMPETUS project consists in a target diagnostic of biological agents in a confined space. This approach can only be used to assess the risk associated with living organisms (toxins and viruses are excluded). Indeed, until now, after concentration on a filter, the sample was brought to the laboratory for analysis and specific research of certain bioterrorism agents. This methodology is difficult to transposed to the field and to a smart city.

Here we offer a regular measurement of the biomass in the air using ATPmetry.

The ATPmetric technique, based on the principle of bioluminescence, does not require heavy equipment. This technique measures the amount of ATP present in the sample. Indeed, living organisms use ATP as their primary source of energy. The bioluminescence reaction, catalysed by luciferase with the presence of magnesium is as follows:

ATP + luciferin + O2 → AMP + PPi + oxyluciferin + light

The light detected by a luminometer allows the ATP detection in the sample. It was established that when the total biomass is considered, each bacterial cell contains an average of 1 femtogram of ATP [40]. Thus, assessment of the total microflora contained in the sample is possible after lysis of microorganism and ATP release in the medium. This analytical method is very sensitive, with detection limits around 100 bacteria/L and can be easily used on the field, but no study describes its use for bacteria detection in the air. Upstream of the analysis, a preconcentration will be carried out. Two solutions are envisaged: the filtration and the impingement.

Filtration: Microorganisms are retained on the filter while the air is drawn through the filter. The filter can be a fibrous material or a membrane. This method of capture is very effective and yields of 100% can be reached [41]. However, this technique leads to desiccation of bacteria which prevents from doing the analysis by culture [42] [43]. This problem can be avoided using gelatin membranes that limit the phenomenon of drying of microorganisms [44]. The main advantage of filtration to collect microorganisms is the possibility to use molecular methods, such as qPCR or ATPmetry for analyses.

Impaction on liquid media (Impingement): The air is drawn inside a liquid which retains microorganisms. In these devices, bacteria are subjected to high shear that enable separation of aggregates [45]. This technique is one of the less lethal to microorganisms and has the advantage of allowing multiple sample analysis: culture, DNA extraction, microscopy or cytometry. Among biocollectors based on this process, three are the most frequently used: BioSampler (SKC Inc.), Coriolis (Bertin Technology) and CIP 10-M (Arelco). Mathieu et al., 2009 [46] compared these devices and showed that the BioSampler reached collection yields of almost 100%, while the Coriolis was only around 4% and the CIP 10-M around 1%. The BioSampler is however rarely used on the field because of several factors as for example a need of power supply or a fragility of the glass. Therefore, devices with low capture yields are more often used. Finally, these impingers, available on the market, have other significant drawbacks such as high prices and patent protection.

The following table presents the characteristics of the 2 methods:

Table 5. Characteristics of two envisaged solutions for Biochemical Risk Detection

Principle	**Capture Efficiency**	**Biological Efficiency**	**Cutoff diameter**
Impingement	Bacteria: 20%-90% Fungi: 70%-90%	30%-80%	Not described
Filtration	Bacteria: 0%-90% Fungi: 0%-90%	<10%	<0.6 µM

Several factors will be evaluated to assess these two solutions. It will probably be necessary to find a compromise between concentration efficiency in our conditions and the feasibility of integrating the method to perform an online analysis.

The second challenge will be to define the level of contamination. It seems difficult in the approach to consider outdoor environment and we prefer to focus on public indoor environment.

Given the technological gap in air analysis and the prevention of biological attacks, our approach will focus only on living microorganisms (bacteria and fungi) and not on viruses and toxins.

For a public building room, the approximative threshold must be below to the warning threshold (conformity), 100pg/m^3. However, this rate must be moderated in function of some parameters: the number of persons present in the building and the flow of people, the ventilation, the temperature etc… The definition of 2 thresholds (threshold of vigilance and alert threshold) per location is therefore necessary. If one of these thresholds is exceeded, the realization of new sampling on site and the sending to the laboratory to carry out targeted research could be performed.

Another challenge will be to send data to the platform. It will be necessary to define which kind of data will be sent, to propose the better integration in the decision making. Data could be just a value or an information in relation to the threshold overruns.

4.2 Case studies and real-world incidents

In this section we provide a list of case studies and real-world incidents that can be linked to security and safety solution, and gaps and challenges.

4.2.1 Ransomware Attacks.

In March 2018 city of Atlanta, Georgia was the subject of ransomware attack SamSam that breached its network servers and barred more than 8000 workers from the access to the critical records [47]. The attack came unexpectedly and silently started propagating throughout the Atlanta's computer systems [48]. It affected almost half of the city's departments by completely shutting down networks and forcing employees to return to paperwork. Furthermore, the attack thwarted travellers from using Wi-Fi on the Atalanta airport, which is the busiest airport in the world. Even a few weeks after the attack took place, several systems remained unusable and a large number of historical records were in disarray. Perpetrators behind the attack who demanded \$51,000 were identified as SamSam hacking crew, led by two Iranian hackers. They exploited Atlanta network vulnerabilities and outdated computer systems. After entering the system, the hackers gained administrator rights and took control of the servers and files without authorization [49]. Even though the attack was not particularly sophisticated, it highlighted the weaknesses of Atlanta's IT department, including the lack of basic security features and no plan for dealing with the attacks. Later in 2018 and 2019, several similar attacks targeting cities of Baltimore, Maryland, Riviera Beach, Florida and Johannesburg, South Africa also took place [50]. A cyberattack occurred on Friday, November 15, 2019 at the Hospital (CHU) of Rouen (France). The attack would well be of criminal origin. For the moment, the responsibility of any State is excluded. "The software which has blocked all the systems is a software whose purpose is criminal. It has spread in the classic office automation of the hospital, but also in the systems allowing to make medical imaging, analyzes", said Guillaume Poupard, director of the National Agency for the Security of Information Systems (ANSSI), on France Culture on November 24, 2019 [51]. In September 2020, the University Hospital Düsseldorf (UHD) suffered ransomware attack which caused system and data access failure, which in turn prevented medical staff from providing emergency care to patients. Ultimately, this resulted in a death of older female patient [52]. In the aftermath, interest in smart city security started rising and majority of the governmental entities in the USA started taking precautions for defending against the future cyberattacks.

- Relevant Gaps: G1, G2
- Lessons Learned:
  1. Governments should develop policies for managing potential attacks and plans for the fast recovery [53]
  2. Governments should invest more resources in installing required and updating outdated security features of the smart cities. Moreover, portion of the budget should be allocated for data backups and team exercises.
  3. Government employees, leaders, and everyone else involved in the development of the smart cities should be properly educated about the risks of the cyberattacks and ways to prevent them.
  4. Governments should participate in collaborations with academia and education partners in a way to provide students cybersecurity trainings and the employment opportunities.

4.2.2 Human performance issues

"Human error" is a label often used to refer to something having been done that was "not intended by the actor; not desired by a set of rules or an external observer; or that led the task or system outside its acceptable limits". It is based upon the principle that every time a task is performed there is a possibility of failure and that the probability of this is affected by, for example: distraction, tiredness, vigilance, mental workload – to varying degrees and which have a significant effect on performance. For example, high or unbalanced mental workload causes: a narrowing span of attention, an inadequate distribution and switching of attention, forgetting the proper sequence of actions, an incorrect evaluation of solutions, slowness in arriving at decisions. Most examples can be found in the avionics domain (find a list of examples here [54]). Probably the most interesting examples relating to the operational control centres in Oslo and Padova are so-called Air Traffic Control environments. For example, while controlled by the ACC of Zurich, Switzerland, TU-154 aircraft of Russian Bashkirian Airlines and B757 cargo aircraft of the U.S. DHL were flying on a collision course at the same altitude (FL360). Both airplanes descended to avoid each other, then the Bashkirian aircraft collided at a right angle with the Boeing cargo aircraft at FL354, killing all 71 passengers. Major causes: ATC instruction error, RADAR malfunction (Short Term Conflict Alert), Route congestion. Shortage of ATC manpower [55].

- Relevant gaps: G3
- Lessons learned: various aspects of the operational environments' socio-technical systems (e.g., organisational, technological) can combine and have an unintended negative impact on human performance. Section 5 below investigates such issues in greater detail.

4.2.3 Electronic Communications Limitation and Lack of Interoperability

The public safety emergency brought about by the 9-11 terrorists the attacks on New York City's World Trade Center was responded to by 200 units from the New York City Fire Department (FDNY) and emergency units and aviation units from the New York City Police Department (NYPD).

The FDNY response was hindered by unreliable communication between chief officers and firefighters. Communications problems included hand-held radios that did not work well in high-rise buildings, inoperable repeaters, and radio traffic congestion.

An additional problem was that the fire and police teams deployed to the World Trade Center with separate command posts and incompatible communications radios. As a result, observations from the NYPD aviation unit of impending building collapse were received only by police, most of whom escaped the buildings. FDNY personnel did not receive the warnings, and many lost their lives [56].

- Relevant gaps: G4, G6, G7
- Lessons learned:
  1. City emergency services need to plan, exercise, and develop approaches to effective communication between departments
  2. Technical solutions need to provide better interoperability across the needs of various departments and responders, and throughout the range of operating environments.

4.2.4 Biased Automatic Facial Recognition

In January 2020, Robert Julian-Borchak Williams was arrested for shoplifting in Detroit. The basis for the arrest was a match between CCTV surveillance footage and Mr. Williams' driver's license picture. He was detained for 30 hours, after a security guard mistakenly identified him [57].

Because the databases used to train automatic facial recognizers are often predominately made up of white males, these systems are more likely to misidentify women and people of colour [58]. This has led cities in the US such as San Francisco and Boston to ban the use of facial recognition technology by city employees [59].

- Relevant gaps: G3, G5
- Lessons learned:
  1. Automatic facial recognition must be carefully tempered with human judgement
  2. Facial recognition training sets must be expanded to include more women and people of color
  3. Facial recognition technology must be used transparently, in order to gain public trust.

4.2.5 Biochemical Risk Detection

If few deliberate uses of microbial agents, toxins or chemicals substances related to biological or chemical attacks against civilians have been reported to date, some revelations suggest that this kind of attack is possible. Indeed, it can be cited:

- the Aum Shinrikyo (the Japanese cult responsible for the sarin gas attack in the Tokyo subway system in 1995) has revealed the multiple occasions with aerosolizing anthrax from downtown Tokyo rooftops.
- the findings of massive quantities of weaponized biologic agents in Iraq following the first Gulf War,
- and the domestic anthrax attacks in the USA in 2001.

Various measures have been taken as a result of these attacks, and to this extent the diagnosis of patients has often been given priority over environmental diagnosis.

At present, the aim is to identify the biological agent after the incident rather than to detect it beforehand.

This is due to the difficulty of monitoring the air and existence of high diversity of agents. Indeed, among the biological agents, potential bioterrorism weapons include bacteria, fungi, virus and toxins. Microbiological agents are classified in three categories [60] according to the ease of production and dissemination and their mortality rate. The categories “A” and “C” attract the most attention as they represent respectively the known organisms (Anthrax, Botulism, Plague, Smallpox, Tularemia) and the emerging organisms. Category B biological agents are less easy to disperse in the environment and have lower mortality rates than Category A agents.

Detection systems must have the following characteristics [61]:

- The detection result must be obtained quickly
- Low sensitivity
- Discriminate pathogens form other biological or non-biological particles.

A lot of device to detect the agents of the category A have been developed with this specification. However, there is no implementation of this device in monitoring systems to our knowledge.

However, the last studies of Dunbar et al., 2018 [62] provide a recent analyse of the situation and underlined the highest priority operational change. This article recommends the abandon of the current concept of city-wide environmental monitoring because the operational costs were too high, and its value was compromised by low detection sensitivity and other environmental factors. Authors give 5 recommendations to increase the resilience and the efficiency on Environmental Monitoring:

1. boost stakeholder confidence by a through validation of system efficacy
2. develop a different approach to sample collection to simplify sample processing
3. develop methods to recover viable agents and functional toxins from aerosols
4. abandon outdoor monitoring and focus on indoor and special event monitoring
5. reduce monitoring costs by developing a reagent-less sensor that can triage aerosol samples in real-time, identifying a smaller set of ‘suspect’ aerosol samples that merit testing with conventional real-time PCR assays

4.2.6 Nation-state attacks

In December 2020, a leading network management software provided by SolarWinds company was compromised by nation-state attackers [63]. The SolarWinds company reported that sophisticated attackers installed malware into their Orion product which may have been installed by more than 17000 public or private sector customers [64]. The affected customers include the US government (finance, health, national security, and telecommunications) and major software companies including Intel. The above-mentioned attack may have allowed attackers to penetrate public or private organization IT systems, steal sensitive information, or install backdoors for espionage purposes.

In the context of smart cities, such attacks are alarming considering the recent trend of nation-state attacks for espionage activities. The resulting stolen data or datasets can be weaponized using Artificial Intelligence to spread targeted misinformation. In addition, such sophisticated nation-state attacks provide a platform to compromise sensitive information handled by popular software or networking tools.

- Relevant gaps: G8
- Lessons learned:
    1. Government needs an effective national and international cyber security strategy for tackling nation-state attacks.
    2. There is a need for cyber security assurance or standardization approach, preferably on national level to meeting certain cyber security requirements for public safety solutions.
    3. Zero trust policy architecture for third party IT software security solutions (handling critical data or assets) should be investigated and encouraged before actual deployments by forming strict national policies.

5 Operational issues

This section focuses on the primary users, i.e., the actors of safety in the cities. Public safety is conducted differently in different cities, but the primary users will typically include actors such as intelligence agencies, preparedness agencies, law enforcement, security contractors, and emergency response agencies. We describe how their work is impacted by the use of advanced technology, in particular how security and emergency agencies prepare for, detect and learn from events; and how these technologies impact processes such as intelligence gathering and sharing, decision-making and inter-agency coordination. Topics of interest also include the new competences expected from operational personnel and managers.

Relying on collection and analysis of data is not new in public safety management. Databases containing images of criminal suspects, fingerprints and DNA are well known examples that reflect the importance of information gathering in policing [26]. But what is different today, as has been demonstrated in the specific examples from Section 2, is the enormous increase in quantity of data and the available technologies to analyse and utilize it for decision support. The threat picture has also changed and safety actors in cities must increasingly prepare for complex events, including hybrid threats and complex coordinated terrorist attacks.

The following sections describe operational challenges that highlight the need for public safety applications and tools, as well as a platform integrating them, in smart cities. The challenges are related to various phases, i.e., intelligence, detection of events, sensemaking/situational awareness, decision-making, and intervention, as well as the more generic issue of coordination. A sub-section is also included on the issue of operational risks in introducing new technology.

5.1 Intelligence

Intelligence in the context of law enforcement and military agencies is usually ordered by decision-makers. Thereafter the intelligence staff develops an intelligence collection plan. After this follows a phase of collection from different sources and by different disciplines of intelligence. Processing and analysis of the findings are then disseminated in an intelligence product which is in turn presented back to the decision-makers. Different disciplines of intelligence can be part of the collection phase. A few examples are human intelligence (HUMINT), imagery intelligence (IMINT), electronic intelligence (ELINT), signals intelligence (SIGINT), open-source intelligence (OSINT), Measurement and signature intelligence (MASINT), Cyber Threat Intelligence (CTI), Geospatial intelligence (GEOINT), and technical intelligence (TECHINT)[1]. In most cases the intelligence agencies are organized at a national level.

A range of challenges can be found related to intelligence work for ensuring the safety of cities and urban spaces. Common challenges are data overload and redundant information, access to information, coordination of information, providing targeted intelligence and putting the intelligence into context.

5.1.1 Redundant information and data overload

A common challenge for the intelligence analyst is the issue of data overload. David Woods defines data overload as: "a condition where a domain practitioner, supported by artifacts and other human agents, finds it extremely challenging to focus in on, assemble, and synthesize the significant subset of data for the problem context into a coherent assessment of a situation, where the subset of data is a small portion of a vast data field [2]." Whereas the goal of the intelligence analyst would be "focusing in on the relevant or interesting subset of data for the current problem context [2]."

Intelligence analysts are challenged by having to monitor systems that are complex and interconnected under time pressure. Moreover, intelligence analysis is a socio-technical domain which requires significant expertise and the consequences for failure are high [2]. The trend in the field of intelligence in the recent years has been an increase in data. Lund Petersen and Schou Tjalve argue that this is partly a result of a more elusive, borderless, and uncertain threat environment [3]. In an attempt to manage the uncertainty, there has been an inclusion of private and civilian data contributors which has led to an expansion of the intelligence collection [3]. New technological collection tools have also contributed to the increase in data. David Woods argues that the waves of technology have "exacerbated, rather than resolved, data overload [2]."

There is a paradox in this issue, since intelligence analysts agree that access to more data is beneficial to the intelligence analysis [2]. However, in practice "the sheer volume of the data creates a situation where it is

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

difficult to determine where to look in the data field, it becomes easy to miss critical information, and determining the significance of data in relation to the ongoing context is challenging [2]." Furthermore, studies of supervisory control domains show that excessive amounts of data increase cognitive burdens for the human operator [2]. In addition to placing an increased cognitive burden on the operators and analysts, it also slows down their work [4]. Without appropriate technological tools for analysis (e.g., AI based analytical tools) the analysts are not able to take advantage of the avalanche of data.

5.1.2 Access to information: darknet, social media and chat applications

Another challenge to the intelligence field is the access to information. The development in the recent years of hybrid threats combining traditional threat factors with factors in the cyber realm makes access to darknet and social media intelligence sources crucial. The characteristics of hybrid threats can be described as: “several tools are used both simultaneously and strategically for maximum effect; and the cyber dimension, along with the social media (SM) and virtual realms offer new, inexpensive avenues of attack [5].” Hybrid threat instruments can include propaganda spread by traditional and social media, fake news, strategic leaks, funding of organizations in other countries, support of political parties in other countries, organizing protest movements via social media, cyber tools used for espionage, attacks and manipulation, economic leverage, the use of proxies in unacknowledged wars, and paramilitary organizations [5]. Since these methods and tools are often non-military and operate outside and below detection thresholds, they represent a new type of complexity for the intelligence community [5]. The recent storming of the Capitol Hill (January 2021) highlights the need for safety actors in cities to prepare for this type of threats.

Access to intelligence from darknet, social media sources and chat applications can prove vital in detection of terror attacks as well. These channels are used by terrorists and extremists alike in planning and coordinating attacks. The report written by the commission investigating the 2015 Charlie Hebdo/Hyper Cacher and 13 November attacks in Paris (including the Stade de France explosions, the bar and café shootings and the Bataclan massacre), highlights the pre-event intelligence failure and attributes it to lack of expertise and technological means. The perpetrators went under the radar of the intelligence services during the planning phase due to sophisticated communication methods. Especially mentioned was the use of darknet and chat applications such as Telegram [6].

Moreover, the darknet, social media networks and chat applications are used for other types of crimes, such as drug and weapons dealing, selling and spreading of sensitive information, digital economic fraud, sharing and broadcasting of sexual crime related material and more.

5.1.3 Access to information from other intelligence agencies and disciplines

Access to information can also be a challenge since different intelligence agencies using different intelligence disciplines and sources are commonly situated at different locations and have limited information sharing between them. This leads to a lack of sharing of raw data, but it also complicates the coordination of analysis [7]. Each agency has their own pieces of the puzzle, and they might not be aware that another agency has retrieved another piece of vital intelligence. This complicates the ability to see the overall threat picture.

Failure to combine leads or signals from different sources can have serious consequences. Prior to the 22 July 2011 terror attack in Oslo and at Utøya, the lone wolf terrorist Anders Behring Breivik bought large amounts of fertilizer and three weapons, while at the same time engaging in extremist forums online. This information was not picked up and combined by the Norwegian Police intelligence services (PST). Behring Breivik thus went under the radar of the national intelligence services. One of the reasons was that PST had not yet developed sufficient capacity and expertise on open source intelligence (OSINT) (p. 391) in [8] and [25]. OSINT became a highly prioritized area in PST in the aftermath of 2011 [25][24]. Another reason was that the register responsible for purchases of fertilizers that can potentially be used to produce explosives did not share this information with PST, and there was no routine for such information sharing [8].

Hulnick [7] similarly attributes the intelligence failure of 9/11 and the failed estimate on Saddam Hussein's Iraq's nuclear bomb capacity to lack of coordination between different intelligence agencies and intelligence analysis based on too few and unreliable sources.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

A co-location of operators and analysts from different disciplines or agencies is often suggested as a possible solution to the issue of inter-agency information sharing. However, experience has shown that a physical co-location does not necessarily solve the issue entirely. The 9/11 investigations concluded that "the then existing counter-terrorism center (CTC) was not a place where all information was shared [7][7]." A digital co-location in the form of a common platform for collection and analysis can be another possible solution to this challenge and can contribute to increased information sharing in real time.

5.1.4 The challenge of providing targeted and relevant intelligence

Another challenge for the intelligence field is how to provide targeted and relevant intelligence. The intelligence actors are challenged by dynamic threat pictures. These change over time and differ in different locations. To be able to predict and plan for possible scenarios, intelligence actors need to follow the developments closely and try to foresee the crime and security related trends.

Intelligence collection and analysis cannot be seen as a mere neutral and technical activity that operates separately from society [13]. As put by Lutsch [10]: “[A]nalysts are like people assembling a jigsaw puzzle who have some nifty secret nuggets inside a box but need to see the picture on the cover to understand how they fit. That picture is drawn by many, including academic researchers, think tanks, the media, and others". Thus, the job of the analyst is in part to evaluate raw material and put it in perspective[7], but part of the job of the analyst and the intelligence managers is also to evaluate from which topics and sources to focus the collection. Intelligence collection can be ordered by policy makers based on what they deem as prioritized threats (national threats and interests), however in practise it is often the intelligence managers who determines the direction of the collection based on the context, former experiences, and previous intelligence productions (i.e., "filling in the gaps") [3]. Intelligence and analysis thereby operate in parallel and are integral processes[3][3].

The overall context and developments on a societal level is thus always important both for intelligence collection and analysis. As argued by Herbert in Petersen and Tjalve "methods used for assessing threats and risk can help to ensure against bias and validate the information which increasingly comes from diverse and external sources [3]." In the case of the security of cities, threat assessments and mapping of threat actors and possible targets allow the intelligence actors to focus their collection on the most likely threat actors. Furthermore, mapping of the soft targets within a city, as well as the main threat actors and their specific target groups can heighten the preparedness for attacks, different types of security related events and different types of crime.

To summarize, operational issues related to intelligence thus include:

- Redundant information and data overload.
- Access to information: Darknet (such as TOR), Social Media and Chat Applications.
- Access to sources from different intelligence disciplines and inter-agency communication.
- The challenge of providing targeted and relevant intelligence through collection and analysis.

5.2 Detection of events

There are different operational challenges connected to the detection of events. Among prevalent ones are operators’ attentional challenges in connection with monitoring CCTV, sensors, traffic and movement of people. In the detection phase there is still uncertainty about the nature of the event, and therefore we also address the issue of preparing and training for detection and response during uncertainty.

5.2.1 Attentional challenges

Among the main challenges involving the detection of events are the ones relevant to attention and noticing anomalies. Operators monitoring closed circuit television (CCTVs) are challenged in this respect. They typically must pay attention to multiple screens simultaneously over a prolonged period. CCTV surveillance is an attention demanding process, requiring "selective, focused, divided and sustained attention." The fact that sustained attention or vigilance tasks place high demands on mental workload is well established [11].

As with task engagement, there is evidence of detection performance decreasing over time (i.e., vigilance decrement)[11]. Vigilance is "critical for monitoring tasks that require intense and sustained attention, because as time goes on, this attention wanes and detection of a person, object or other change in the environment becomes less likely or slower". This is known as the vigilance decrement, which typically occurs after 20 to 30 minutes of continuous work [20]. Furthermore, both work overload and underload can have negative consequences and lead to mistakes being made in the control room [20].

The same challenges apply to operators manning other functions in control rooms. This could be operators supervising different types of sensors (e.g., air sensors, biochemical sensors) and operators monitoring movement of people, traffic and more. This kind of work thus challenges the human attention span and the ability to focus and spot irregularities and anomalies in real time. Therefore, technologies that assist the operators in detecting anomalies in these disciplines can improve performance. Moreover, a human machine interaction supervision tool can help determine if an operator has too high workload, or if he/she has reached the maximum for the attention span. This can help ensure the right manning of personnel for the right tasks at the right time.

5.2.2 Preparing for uncertainty: detection and response

During recent years, terror attacks have become more complex and sophisticated. The attacks have a predominantly urban character, and the tactics are multifaceted aimed at inflicting maximum damage, while at the same time hampering the work of first responders. In the intelligence community "complex, unpredictable and asymmetric threats of terrorism, cyber-attacks and other organized crimes have increased […] focus on how to prevent and prepare for the unknown catastrophe [13]." Preparing for such scenarios and understanding the pre-event signals represent an operational challenge for safety actors in cities.

A new type of terror attack categorized as complex coordinated terrorist attacks (CCTAs) by the U.S. Homeland Security represents challenges for planning, training, and detection. Usually, CCTAs include multiple teams of perpetrators, as well as multiple attack locations and weapon types. A few examples of CCTAs from recent years are the train bombings in Madrid 2004, the train and bus bombings in London 2005, the Mumbai terror attack in 2008 (firearms, bombings and arson), the Paris 2015 terror attacks (firearms and bombings), the Brussels 2016 airport and train bombings, the Alexandria/Tanta 2017 church bombings and the Barcelona 2017 vehicle ramming and knife attack [12].

CCTA perpetrators tend to select soft targets and vulnerable environments in order to maximize casualties. They also attempt to strike multiple targets simultaneously and quickly or in close succession before they move to another location. Other types of targeted attacks of violence might mimic CCTA tactics and will demand the same level of management and coordination [12]. Preparing for CCTAs demands training for and preparing plans for detection and response to multi-location terror attacks, by multiple weapon types. In Germany a new police training module including a public and urban component has been introduced after the terrorist attacks in Paris, Nice and Brussels "aimed at strengthening the capabilities of the police to respond to situations of violent mass attacks – situations whose 'specific' forms are not predictable, but that share the 'essence' of disrupting urban life by hitting key infrastructures and killing many, with offenders ready to die in the process [13]."

The focus points of the new training program include preparing for an instant and complex situation and for the interaction between agencies involved in such a scenario. Furthermore, it prepares the participants for "the need to be aware of what is and what might be, to act instantly, smartly and collectively at the scene of an attack [13]." Krasmann and Hentschel, argue that the future-oriented demands of prevention and pre-emption will include the need for "alertness, smartness, sensitivity and prompt reactions in the here and now [13]".

To summarize, operational issues related to the detection of events thus include:

- Attention challenges for operators manning different types of control rooms.
- Human machine interaction.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

- Preparing and training for detection and response during uncertainty and unexperienced scenarios.

5.3 Sensemaking and situational awareness

After the detection of an event/anomaly follows a stage of sensemaking and situational awareness. Part of the process is understanding the nature of the event and combining information from different sources, actors and agencies.

Having situational awareness is crucial for law enforcement and first responders once a situation is ongoing. The strength and capacity of the perpetrators is for example central when law enforcement is organizing the resources and tactics for an intervention. For law enforcement personnel or soldiers, situational awareness is also part of being alert and prepared and having the ability to read the surrounding environment and correctly assessing the signs of danger. The goal is to react with "a temporal and tactical advantage" against the adversary [13]. Sensemaking is equally important when an ongoing situation has been detected. Berlant, Krasmann and Hentschel define sensemaking as "a range of sensing skills needed to grasp situations, that is, to know what they are and 'how to be in [them]' – or else, how to get out of them [13]." In order to understand the situation, the safety actors will have to sense, perceive, read, assess, guess or conjecture a situation. Using one's senses, such as touch, smell, and vision, combined with the use of technological devices and algorithms is also part of sensemaking [13].

During the 13 November 2015 attacks in Paris law enforcement and first responders alike were challenged by a complex threat picture that occurred with no warning since there was no intelligence foreseeing the attacks. This made situational awareness and sensemaking difficult. In the case of the Bataclan attack, the report by the investigating commission paints a picture of confusion both at ground level and at the coordination level. When the special forces (FIR de la BRI de Paris) arrived at the scene about one hour after the onset of the attack they had little knowledge about the situational picture inside the building. It was unclear whether the terrorists were still inside the building, whether the hostages were trapped with explosives, if explosives were hidden, or if the terrorists were planning an ambush (p.59) in [6]. Further confusion derived from the fact that it was a multi-location attack with three different main venues. The victims who were able to flee the different venues involved in the terror attack hid in numerous locations, and then called the police. This led to confusion about how many attacks there were and their exact location. It seemed to the police at the time, that more locations were involved than what was the case (p.56) in [6].

The lack of situational awareness made the mission of the first responders less efficient and more hazardous. The reason for the lack of situational awareness could be multifaceted. It is not clear whether it was lack of information from inside the building, or the failure to retrieve, coordinate or correlate the information. It could also be due to lack of proper technological means, such as CCTV surveillance or timely access to such means.

In the case of the 22 July 2011 terror attacks in Norway, the police had the registration number and characteristics of the perpetrator's getaway car after the first bomb attack at the government building in Oslo. However, they were not able to share this information efficiently within the police (p.21) in [8]. A more efficient sharing of this information could have enhanced the situational awareness of the police personnel involved in the search of the terrorist and perhaps improved the outcome.

Operational issues related to situational awareness and sensemaking thus include:

- The challenge to retrieve, coordinate or correlate information that contribute to situational awareness in the field.
- The challenge of SOC operators to efficiently share information with responders in the field.
- The challenge to make sense of information and observations in the field and make the right assessment of the situation.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

5.4 Decision-making

Decision-making during complex, critical events often imply dealing with several aspects of uncertainty. Situational awareness is key to well-informed decision-making. Still, there are situations in which decisions must be made without all relevant information available at a given time. As an example, the 22 July investigation report explains how the first hours after the bomb in Oslo were characterized by great uncertainty as to what had happened and who was responsible. Just minutes after the explosion, the police realized it was an act of terrorism and that there could be more attacks to come; however, they did not know where. Still, the commission found little evidence of operative measures aiming to prevent or prepare for new attacks (p.452) in [8]. Thus, in this case, the high level of uncertainty may have contributed to the lack of necessary decision-making and actions. Also, the uncertainty regarding whether there were more terrorists on the Utøya island after the perpetrator had surrendered, led to the decision that rescue workers were not transferred to the island meaning that the police had to perform first aid and evacuation.

The investigation report explicitly emphasizes how crisis management involve demanding decision-making situations. In situations where quick action is necessary and many things happen simultaneously, performance is rarely better than the preparations. The commission found that there had been too little training on some aspects, whereas other examples showed that realistic exercises proved important for efficient response (p.452) in [8]. Training related to decision-making during complex and uncertain situations is thus essential.

As also highlighted in the 22. July commission report, most crises involve many actors, all feeling that important interests are at stake. Gaining control of the situation is a matter of urgency, and at the same time ordinary decision-making processes may not be considered adequate (p 209) in [8]. Who is responsible for combining relevant information and making decisions based on that information? That is, it is important to establish clear and unambiguous roles and responsibilities both during normal operations and during crises; and to make sure these are known and understood by all relevant actors. Training plans should be created that include aspects related to decision-making responsibilities in both situations.

Operational issues related to intervention thus include:

- The challenge of decision-making in situations where all information is not available.
- Training related to decision-making during complex and uncertain situations.
- Challenges connected to decision-making responsibilities during both normal operations and crises.

5.5 Intervention

The safety of first responders (firemen, law enforcement, emergency management, emergency medical services, healthcare, and transportation) is always at stake when intervening in an ongoing security event. When speaking of CCTAs it is even more important since common tactics in CCTAs aim to disturb the work of the first responders and inflict damage:

- Among their tactics are efforts "to counter first responders and law enforcement in an effort to increase casualties, inflict maximum damage at attack sites, and prolong incidents to achieve sustained media coverage [12]."
- "Delay or deny exit by victims and entry by public safety by blocking exits and/or chaining/rigging doors with explosives, using tear gas, and/or using fire/smoke to delay law enforcement response efforts and potentially prolong the incident [12]"
- "Take hostages to prolong the incident and/or delay law enforcement response efforts [12]."
- "Conduct secondary attacks on first responders, evacuation routes, and/or additional sites, such as medical facilities, that are part of the response [12]."

During the Bataclan attack, the safety of the fire brigade of Paris (BSPP)[14], doctors and paramedics was a critical issue. The injured had to be evacuated and treated while the terrorists were still present in the building. This challenge was solved by having doctors from Recherche Assistance Intervention Dissuasion

(RAID) [15] enter the building protected by vests and helmets to treat the wounded and prepare them for extraction from the building. The treatment itself and the extraction was covered by armed police (p.58) in [6]. Different police units evacuated the wounded and shocked survivors from the Bataclan to advanced medical posts in the Oberkampf street where the BSPP took over under protection of soldiers from l'opération Sentinelle (p.60) in [6].

The Bataclan incident teaches us how the safety of the first responders was heightened by cooperation between different types of first responders in the field and at the coordination level in a very complex and extreme situation. As mentioned previously in section 5.3, sensemaking and situational awareness can also contribute to increasing the safety of the actors.

Operational issues related to intervention thus include:

- Actors' safety.
- Cooperation in the field and at coordination level.
- Sensemaking and situational awareness.

5.6 Coordination across roles and organisations

"Historically, law enforcement, fire, and emergency medical services (EMS) personnel have viewed their first responder roles as independent of each other. As a result, the first responder community may not be prepared to function as one team to rapidly neutralize threats and save lives [16]." There is, however, an increase in events that require the deployment of all first responder disciplines, e.g., active shooter/hostile events (ASHEs). It is important that all relevant actors of safety are included in defining new ways of working together. With the aim to identify best practices for an integrated ASHE response, the InterAgency Board (IAB) convened an Active Shooter Summit. Participants representing law enforcement, fire, and EMS responders from municipalities in both the United States and United Kingdom, several state and federal agencies, as well as Texas State University worked together in identifying discrete recommendations that were condensed into 10 broader best practices. The first recommendation is for leadership to prioritise and support the development and implementation of proactive ASHE-relevant joint policies, procedures, training, exercises, and equipment [16].

In a report on planning considerations related to Complex Coordinated Terrorist Attacks (CCTA), Homeland Security describes how a CCTA targets multiple geographically dispersed locations to overwhelm a jurisdiction's capabilities. Although law enforcement may have enough resources to stop attackers at one location, CCTAs may introduce new challenges in coordinating the response at multiple locations [12]. Such attacks imply a need for increased and improved coordination not only between different actors but also across geographical locations. The Paris attacks on 13 November 2015 illustrate these challenges as the number of specialized forces available for each location was limited and the right type of first responders and law enforcement for each event were not the first ones to arrive.

An issue that was raised after the 22 July terror attack at Utøya, was the limitations of the logging system, enabling efficient sharing of information between the operators and between operators and staff. The operation central's performance was impaired by the absence of technical solutions that could have made notification and information sharing more efficient. For instance, the operations central did not have systems for effective mass mobilization of own crew or written information sharing with the street police. In the above-mentioned report, Homeland Security argues that a well-coordinated incident command system is critical for an effective response to such attacks, and that since they may occur with little to no warning, "establishing timely communications among and between the affected communities, and all responding disciplines, is critical to an effective response" (p.5) in [12]. Timely communication requires cross-organisational communication channels that are known and interoperable. Interoperability is, however, listed as one in three main challenges in an article on the legacy and emerging technologies for public safety communications [17]. The Office of Community Oriented Policing Services at the U.S. Department of Justice has issued a guide for communications interoperability in which interoperability is defined as "the ability of emergency responders to work seamlessly with other systems or products without any special effort" (p.15) in [18]. The guide discusses challenges and critical elements and provides a step-by-step plan for how to achieve communications interoperability. In a report on interoperability of real-time public safety

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

data, the National Institute of Standards and Technology (NIST) provides an overview over challenges with a focus on data exchange standards, data access control approaches and data sharing policy frameworks [19].

Among its recommendations for integrated ASHE response, the IAB further emphasizes the importance of creating and implementing a common operating language. This best practice includes aspects such as using plain language that enhances communication and response especially under stressful conditions. Terms that are used should promote agencies working together and common language and terms that are agreed upon should be practiced pre-event [16]. It is therefore important that responders using coming tools use a common terminology and symbology.

Operational issues related to coordination thus include:

- Inclusion of all relevant actors of safety when defining new ways of operating.
- Capability challenges during Complex Coordinated Terrorist Attacks.
- Timely cross-organisational communication and interoperability.
- Common operating language including common terminology and symbology.

5.7 Operational risks in introducing new technology

With new technology and tools, the organization of work, the human role and the work tasks will change, and it is important that the organization is prepared to handle the introduction of the new tools. Common weaknesses are ambiguities in roles, responsibilities, and communication [21]. In addition, there may be a low perception of risk and awareness of new challenges [22]. It will be necessary to examine how the new work tasks can be designed so that they take human possibilities and limitations into account. It is often in the unknown and unexpected situations that problems with new tools, technology and work tasks arise. This must be handled at a people-centred level and at an organizational level with interaction between several actors, not just through technology and tool development. Training, confidence in the change process and technology and tools are organizational factors that are important to consider when introducing the new tools. The assumptions and plans that form the basis for new work processes must be in accordance with the competence and expectations of the users, which can be ensured with user-centred development and step-by-step introduction of new technology.

Misunderstandings and errors of expectation can be linked to the design of procedures, the transmission of information between individuals and teams. Training based on situational awareness and human factors can provide better interaction [23].

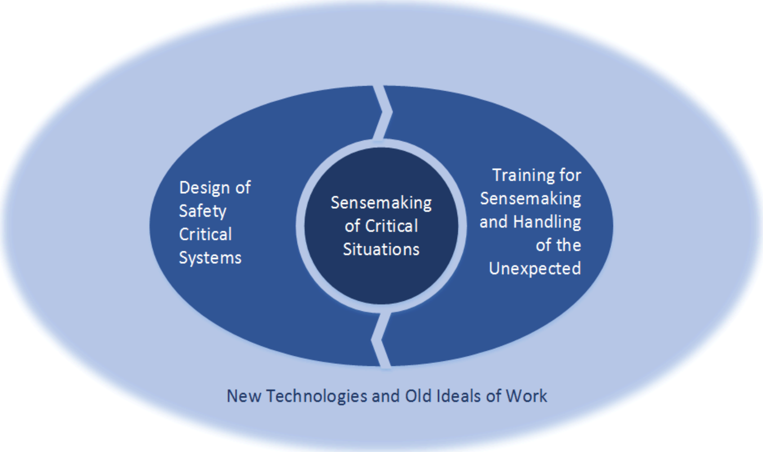
Design of Safety Critical Systems
Sensemaking of Critical Situations
Training for Sensemaking and Handling of the Unexpected
New Technologies and Old Ideals of Work

Figure 3. Sources of impact on sensemaking of critical situations

The following table provides some details about types of issues arising when new technology is introduced in operational environments:

Table 6. Types of issues arising when new technology is introduced in operational environments

(Wrong) assumptions about the organisation of operations	• Inter-organizational complexity- all organizations will have different special preferences, ways of working etc. that will affect how they work with the platform. • Information is interpreted differently by different actors. This demands common terminology and framework. • Tailormade plans/interfaces for each user/city are needed. • Division of responsibilities: Who is responsible for which tools in the platform? Who manages the intelligence circle, and who makes decisions?
Need for new competences	• Not fully understanding all necessary competences. • Difficult to train and prepare for situations that have still not occurred. • Change of attitude is needed to adjust to new work tasks. • Training is needed for all likely scenarios and conditions.
Impact of technical failures / unavailability of service on operational capacity	• AI can miss vital information (human needs to be in the loop). • Not being able to share information effectively. • Can one still operate without the technology or in degraded modes?
Relying too heavily on AI to detect events, etc.	• AI should ease the workload of the operator; however, it will not be able to do all the analytical work for the operator (human needs to be in the loop). • Operational risks connected to the social media and darknet analysis part of the tool. The operator needs technical knowledge about how sources are monitored or collected, and the societal context. • Operational risks connected to biased AI based video analysis (face recognition and weapon/anomaly detection) could be informed by prejudice and reinforce stereotypes. • The operator should understand underlying AI calculations/possible outcomes.

5.8 Learning from events: summary

This section summarized some of the main technology and organizational related learning points of recent security events. These points were used in the previous sections to illustrate challenges related to the different aspects and phases of public safety operations:

Table 7. Summary of operational learning points from recent public safety events

The 22 July 2011 Terror Attacks in Norway[8]	• The operations central lacked an overview of available police resources. • Initially, fleet management via Geopol (Police maps) was not possible. Hence important tools for efficient management and utilization of own resources were not available. • The operation central's performance was further impaired by several inappropriate technical solutions, as well as absence of technical solutions that could have made notification and information sharing more efficient. E.g., the operations central did not have systems for effective mass mobilization of own crew or written information sharing with the police officers in the field. • The logging system (PO) had limitations that did not enable efficient sharing of information between the operators or between operators and staff. • Insufficient police helicopter capacity and deficient coordination with the army about the use of military helicopters led to a late helicopter response.
London/Manchester (2017) [27]	• The need for a better strategy for acquiring, analysing, and sharing data across intelligence and policing, for example through wider use of bulk personal datasets and by enhancement of tools. • The need for improved flow of information in both directions also has the potential to contribute to better decision-making at the centre in relation to the risk from closed SOIs in particular. • A need for continued focus on the challenges posed by encryption. • A need for increasing cooperation with the private sector, for example to improve the detectability and even the preventability of purchases of potential explosives precursors by would-be terrorists, as undertaken before the Manchester and Parson's Green attacks.
Drottninggatan, Stockholm (2017) [28]	• The police did not have appropriate tools available for sharing of images across the organization. • The batteries of several of the radio communication units died, leaving some of the police officers with no way to communicate. • The police authority needs to find better ways to share information and communicate. • There is a need for better tools to share and analyse large amounts of data.
The France 2015 Attacks[6]	• The need for new technical tools for intelligence gathering. • The variety of new communication methods for terrorists and the need for new ways to monitor these communication channels was addressed in the report investigating the attacks. • The report recommended the intelligence services to develop structures for analysing information from the darknet and to recruit more high-level experts in this field. • Challenges connected to a multi-location attack were described in the report. The number of specialized forces available for each location was limited. The right type of first responders and law enforcement for each event was not the first to arrive at the scenes.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

6 Ethical and legal issues

The purpose of this section is to examine potential ethical and legal requirements relevant both in IMPETUS Project's context and in broader considerations. This section constitutes the ethical framework's initial considerations (WP5). The ethical framework in question analyses the implications of current capacities in data gathering to the personal data rights in the context of security and intelligence data-gathering operations. This section and the ethical framework will not assess the ethical issues associated with the pilots and other data collection activities during the IMPETUS project (this constitutes a separate case and is the responsibility of WP8; see Ethics and data protection, 2018).

The concept of a smart city, among others, includes tools and methods to enhance urban areas' security (Clever *et al.*, 2018; Vogiatzaki *et al.*, 2020). One typical example of an intelligent security hub is the City Office of Homeland Security, in the City of New Orleans (New Orleans, 2021), United States. The system pulls live feed from 400 city-owned and 150 business-owned and private homes-owned closed-circuit television video surveillance systems (CCTV)s. The system is connected to the emergency telephone service, with the built-in automatic screening of all locations relevant to incoming emergency alerts or calls for assistance. Thus, the system allows immediate real-time visual access to the emergency location (*situational awareness*) before emergency service arrival. Also, it enables historical footage, which is particularly relevant for investigatory purposes (*investigation enhancement*). The Artificial Intelligence (AI) system utilized by the real-time crime centre is an advanced machine learning algorithm capable of analysing the recorded footage without human interference (*descriptive artificial intelligence*). It offers advanced identification methods in real-time and historical footage (including surveilled targets' *behavioural aspects*; Timmermans (ed.), 2009).

The AI system is *non-stop* active (*non-stop surveillance*). The algorithm learns to recognize and separate normal from unusual behaviour/motions in specific areas/circumstances by monitoring the stock footage. The data collection is thus enhanced. A real-time footage recording is analysed, allowing subject profiling (*subject profiling*; the so-called *laser analysis*: behavioural patterns, associations, property, interests, and others).

A question is raised to what extent the AI algorithm is in charge of recognizing suspicious occurrences and altering human operators' perception of suspicious circumstances. This issue is related to concerns regarding the use of algorithms (and bias) in *crime prediction* and *facial recognition*, *predictive policing* in general, *place-based predictive policing* (*high-risk areas crime patterns*), and the notion of *pre-emptive justice*. The data utilized to generate early profiles is based on the already existing data in police records. This practice theoretically enabled the transfer of the established police record bias (the so-called *over-policing* in areas usually characterized as minority areas, low-income areas, and similar) into AI algorithms (Ferguson, 2017).

With the advancement of technology, the body-worn cameras and other smart devices (the so-called connected police officers) and drones (utilized by police) will easily incorporate the AI technology. Besides, the AI system will become increasingly interconnected with various data sources (*Security Internet of Things*; i.e., license plates registry, parking systems, hotel registrations, transport systems' datasets, other publicly and privately owned CCTVs, various sensors, social networks, and others). The social network data set is particularly data abundant. Besides the usual exchange of posts and messages, the *metadata, cookies, web scraping,* and *text mining* can reveal identifiable data, such as user information, user location, and more (Menzer *et al.*, 2015). The described technology, to a large extent already employed in practice, brings the surveillance and information-gathering capabilities to a new level. Such a database is continuously growing, incorporating information on surveillance targets and many other individuals not necessarily to any extent a part of criminal investigations.

6.1 General considerations

6.1.1 Socio-technical environment

Whereas the public, in general, supports the primary efforts aimed at enhancing public security, the data-collection technology utilized in security operations may raise concerns about privacy issues. The timely and efficient law enforcement operations may require intrusions into privacy, thus requiring precise and detailed analysis of the available ethical and legal guidelines and rules on how the engaged actors must handle such

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

data processing. The ethical considerations revolve around the principal conflict of interests between collecting, analysing and sharing big data on one side, and the need to protect personal data on the other. In the context of a smart city, the noted strife is enhanced by the ever-increasing smart city capabilities of gathering big data versus the civilizational strive to promote data rights as human rights (*human-centric* approach). As noted by the European Commission (EC) in 2015 (EC, 2015), it is challenging to balance citizens' personal data confidentiality with the law enforcement and judicial proceedings' transgression into personal data. The purpose of an ethical framework is to reconcile the two, at first glance, opposing forces, and to explore venues of co-existence (**socio-technical environment**).

6.1.2 Involuntary data collection and manipulation

One of the more critical junctions in evaluating the ethical permissibility of data collection and manipulation concerns the instances of automated or (semi-)directed **involuntary data collection and manipulation activities.** These activities include involuntary data collection (i.e., sensors, CCTV cameras, smart devices, and similar), involuntary identification (i.e., face recognition, biometric data, automatic voice detection, and similar), involuntary tracing and tracking, and the consequent analysis of such data. The noted activities are relevant concerning the person whose device is being accessed and all individuals whose data is captured by such a device.

6.1.3 Mass surveillance

The all-out collection and manipulation of data are particularly pronounced in the differentiation between targeted surveillance versus mass surveillance (Cate, Dempsey (eds.), 2017). Indeed, the IMPETUS Project is focused on the **mass surveillance** enabled through smart city public and private surveillance devices and driven by the AI algorithms that are able to make sense of big data coming in.

In the context of modern security challenges, it would be irresponsible to neglect and abandon the means and tools in data mining and analysis offered by the AI (EC, 2020b). At the same time, it will be necessary to understand what makes the mass and targeted surveillance justifiable and what are the concrete benefits of employing AI algorithms in such operations. This evaluation's outcome must have a fair and beneficial effect on the security and intelligence sector and society. A positive impact on society (***common good*** *principle*) must outweigh all negative aspects (von Silva, Larsen, 2011). Potential threats and risks (internal/external, intentional/accidental) must be acknowledged and mitigated to the best extent possible (*maximization of opportunities and minimization of risks principle* (Floridi *et al.*, 2018).

6.1.4 Common good

The common good principle should point to a particular value of general appreciation that gives justification for reducing other values, principles, and rights. In the IMPETUS Project's context, principally focused on what the European Data Protection Supervisor (EDPS) referred to as the so-called *big data protection ecosystem* (EDPS, 2015), the focus is placed on the notions of **privacy** and **personal data**.

6.1.5 Privacy and personal data

The Convention for the Protection of Individual with regards to Automatic Processing of Personal Data (APPD, 1981) with its latest Protocol from 2018, recognizes the need to assess the protection of personal data keeping in mind the "… *diversification, intensification and globalization of data processing and personal data flows* ..." (APPD Protocol, 2018: Art. 1(2)). The APPD Protocol recognizes the need to reconcile the right to personal data protection with other fundamental human rights, thus **elevating the data rights to the fundamental rights' core echelon**. The personal data implies any information pertaining to an identified or identifiable individual (Art, 1. APPD; co-opted by the General Data Protection Regulation (GDPR; GDPR, 2016) in Art. 4(1)), irrespective of its nature (WP Article 29, 2007). The term identifiable may relate to anonymized data that can be re-personalized. Keeping in mind that any kind of data can be adjoined to the personal data category (including items such as the metadata, the IP address, and similar), a large section of big data collection and manipulation pertains to the noted category (Voigt, von dem Bussche, 2017:240 *et seq.*). It should be pointed out that the non-personal data is regulated by the Regulation (EU) 2018/1807 on the non-personal data (Regulation (EU) 2018/1807, 2018). The noted Regulation, among other items, gives precedence to GDPR when the personal and non-personal data are contained in one data set.

The right of privacy, recognized as a universal human right by the Universal Declaration of Human Rights (Art. 12; UDHR, 1948), is, among other sources, defined by the European Convention of Human Rights (Art. 8; ECHR, 1953). The Convention (as interpreted by the European Court of Human Rights) places an obligation on the State to **protect its citizens against unjustified intrusions into their private affairs**. Such intrusions are only permitted if prescribed by law and required by exceptional circumstances (i.e., national security, prevention of crime, citizens' protection, and similar). Such exceptions are scrutinized by the Court of Justice of the European Union (CJEU), particularly regarding the data protection defined by the Charter of Fundamental Rights of the European Union (CFREU, 2012).

Limitations and exclusions

CRFREU requires (Art. 8) consent for data collection or some other legitimate basis and stipulates the subject's right to access collected data and the right to rectification. In cases where such rights are to be limited or excluded (Art. 52), the limitations or exclusions must be **prescribed by law**, must be **necessary** (sufficient grounds) and **proportionate** (choice and severity of measures), must be **foreseeable** (to a certain degree), and must **fulfil broader goals of general interest** (in the **public interest**). The APPD Protocol reinforces the afore-mentioned criteria by stipulating (Art. 14) that any data processing activities justified by **national security** or **defence purposes** must be subjected to a regulated independent review and supervision. GDPR also stipulates several legal grounds (Art. 6(1), Art. 10, and others), including the public interest and the **exercise of official authority** (Handbook, 2018). Art. 23 GDPR details several reasons for a valid exclusion or limitation of subject's rights, including national security, defence, **public security**, **criminal proceedings**, critical public interests, and others. Similarly, the Directive 2002/58/EC on privacy and electronic communications (Directive on privacy, 2009) completely sets its application aside regarding the matters of **state security**, public security, defence, and **criminal law**.

Based on Art. 23 GDPR (and other similar rules and other legal documents), national legislation usually adopts separate acts and statues concerning the **security and intelligence operations**, **criminal proceedings**, **public security issues**, **national security issues**, and others (European Data Protection Board (EDPB); EDPB, 2020). Therefore, the regulated aspects of personal data and right to privacy may or may not be relevant for each jurisdiction, as most relevant rights are either limited, restricted, or altogether excluded (AccessNow, 2019). Indeed, most European Union (EU) Member States and other states will have enacted specialized laws and status concerning the operation of their security apparatus, police force, data secrecy, and similar. In principle, the matters of national security remain under the purview of states (Member States in the EU context; as per Art. 4(2) of the Treaty on the Functioning of the European Union (TFEU, 2012)).

One more important limitation requires mention. The basic foundation of privacy rights revolves around individuals' right to access their data, to control their data, and to decide how their data is being used and by whom, including the right to be informed that their data has been collected and manipulated. The noted foundation might not necessarily be an available option in the context of security and intelligence data collection and manipulation operations. Still, there is some consideration to the contrary (EDPS, 2020:8). Therefore, the **right of information and access** and the previously noted **prior consent principle** must be further examined to determine to what extent, if any, these principles can be applied in the IMPETUS Project's context.

Traceable vs. untraceable data

The GDPR additionally relates to the term pseudonymization (Art, 4(5)), referring to a data management technique whereby a set of data relatable to a particular individual (subject) can only be accessed by using a separate key. This method allows creating two different sets of data, one traceable and consequently re-identifiable, and the other untraceable, not identifiable, and, ultimately, possibly not subject to personal data regulation. This matter deserves further examination in the IMPETUS Project's context.

6.2 Legal analysis

The ethical framework is not to replace the law or public policy. Indeed, the questions at hand do require a separate legal consideration on regulatory and case law steps, as well as industry standards and codes of conduct. Such legal scrutiny is only beginning to emerge (as noted by Asilomar AI principles; Asilomar, 2017). Introducing AI systems into everyday operations will likely require an overhaul of existing legal principles and norms (as indicated in United Kingdom (UK) Parliament Artificial Intelligence Committee, Chapter 8; Artificial Intelligence Committee, 2017; EC, 2020a). The IMPETUS Project requires a detailed analysis of various aspects of privacy, security, and surveillance concerning the involuntary visual and audio capture of personal property, access to personal data, involuntary surveillance, storage, and security of data collected, access to such data, and similar. To reach this goal, it will be necessary to summarize relevant legislation (and, where available, case practice). The ethical framework may be used for general consideration on the *de lege lata* and *de lege ferenda* legislation (Young, Katell, Krafft, 2019, EC, 2019). Concerning the policy consideration, the evaluation of the so-called *digital ethics* (Ethics Advisory Group, 2018) is a helpful tool to both the policymakers and the legislators in considering digital strategies and digital legislation (Evas, 2020; Organisation for Economic Co-operation and Development, OECD, 2020).

The summarized legal analysis will include all the legislation previously mentioned in this Report and several additional legal instruments, as analysed in the further text. The Directive (EU) 2016/680 (Police Directive, 2016), which regulates the (partially) automated processing of natural persons' personal data in criminal investigations and sanctions, public security operations (safeguarding and prevention of crime) law enforcement purposes by competent authorities (public security authorities, other public authorities, as well as private entities statutory entrusted with security operations). The Police Directive follows the GDPR logic (both are a part of the same legislative package) when determining the relevant definitions of terms such as personal data, data processing, pseudonymization, controller, and processor (as discussed above). The Directive establishes several relevant principles, such as lawful and fair processing, legitimate grounds (legality), specific and explicit purpose (necessity), adequate and not excessive (proportionality), accurate and up-to-date, secured and purpose restricted. This Directive is relevant for the IMPETUS Project's context, especially considering the security and intelligence data collection and manipulation activities. It stipulates rules concerning automated individual decision-making, rights of the data subjects (general, information, access, and others), obligations of controllers and processors, data protection officers, supervision, data security, access to data, and data transfer, and others. As is the case with the GDPR, the Police Directive also allows for limitations and exclusions in cases of criminal proceedings, national security, and others, and keeping in mind that this is a directive (unlike the GDPR), the changes of national law variety in regulating these discrepancies and exclusion is increased. The Police Directive includes data processing operations aimed at preventing threats to public security. Additionally, it promotes cross-border cooperation (exchange of data) and establishes a compensation scheme for breach cases (with the general requirements informing the public and individuals regarding data processing).

It should be noted that, depending on a case-to-case evaluation, both the GDPR and Police Directive can be relevant for each security data gathering, processing, and handling operation. The applicable norm depends on who the relevant actors are, how they are involved in the process, and what sort of information is being collected. The noted applicability criteria are of particular importance for private actors who participate in security operations. Private actors could be providing specific services, such as online cloud storage or secure communications, hardware solutions, software solutions, support solutions, and others. Alternatively, private actors could be engaged through public-private partnerships, including a delegation of certain powers and duties to private entities (Purtova, 2018). The noted services must be aligned with general GDPR requirements and, if applicable, particular Police Directive specifications. Also, such activities are likely to be further regulated by other relevant legislation, such as the rules on technical compatibility and security (i.e., Regulation (EU) 2018/389 regarding regulatory technical standards for strong customer authentication and common and secure open standards of communication).

IMPETUS will consider the legal framework established by the Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data. This Regulation is especially relevant because it creates additional rules to those already established by the Police Directive, and are of interest when relevant EU bodies (i.e., Eurojust) conducting law enforcement operations[2] are to be, potentially, adjoined to the IMPETUS platform operations.

[2] With the noted exclusion of Europol and European Public Prosecutor's Office, pending the necessary amendments of relevant acts establishing the noted bodies.

It must be noted that the highlighted legal sources are based on the general requirements and policy set by TFEU (namely Chapter 4 and Chapter 5, Title V, Part Three, TFEU), requiring judicial and police cooperation in law enforcement activities and operations. Furthermore, the European Agenda of Security (Security Agenda, 2015), among other items, highlights the use of several additional legal instruments, including the Directive (EU) 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Directive (EU) 2018/843, 2018), the Directive (EU) 2019/1153 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences (Directive (EU) 2019/1153, 2019), and, Regulation (EU) 2015/847 on information accompanying transfers of funds (Regulation (EU) 2015/847, 2015), allowing the Financial Intelligence Units and other competent public authorities access to sensitive information.

It will be useful to analyse the possible ramifications of the Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (providing clear rules regarding the persons' privacy (i.e., traffic data, location data, secure communication service, and similar; Proposal on Regulation on Privacy and Electronic Communications, 2017), allowing so-called backdoor access by law enforcement and affiliated agencies to individuals' data). Similarly, the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (Proposal on Regulation on Electronic Evidence in Criminal Matters, 2018), as well as the Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (Proposal for Directive on Legal Representatives in Evidence Gathering, 2018), allow for more direct means available to law enforcement and affiliated agencies to connect to individuals' data (Boehm, 2012).

Depending on the relevant stakeholders, the ethical framework may include further legal analysis of instruments such as the Directive 2016/1148 on network and information systems (Directive 2016/1148, 2016), the Regulation (EU) 2019/881 on cybersecurity (Regulation (EU) 2019/881, 201).

6.2.1 Moral machines

One of the central ethical questions in the digital sphere (*digital ethics, big data ethics*) arising from the utilization of AI systems in data collection and manipulation (*AI ethics*) revolves around moral machines and machine ethics concepts (European Group on Ethics, 2018; Corea, 2019: Coeckelbergh, 2020; Zwitter, 2014; Bundesministerium, 2018). These concepts evaluate the AI systems' ability to recognize morally significant situations, recognize relevant values, and factor those values into decisions they make. In the IMPETUS Project's context, the relevant issue to be examined concerns the question of whether values alignment can be conceded to the machines (*AI autonomy* principle) or is that a point where a human operator should take over the data collection and manipulation.

As the Ethics Advisory Group with the European Data Protection Supervisor suggests (Ethics Advisory Group, 2018), the *digital move*, initiated by digital exponential innovation and societal implementation, leads to several undesired effects. The transformation from *real-life subjects* towards *digital subjects* emphasizes digital characteristics, with the moral, cultural, religious, and other constructs falling behind. Indeed, core components of political and social life are slowly transferred to the digital arena, and societal solidarity and empathy are taken over by algorithm evaluation and scoring mechanisms. The Group concludes that moral values, human dignity, and personhood must remain an integral part of any decision-making relevant for data collection, data manipulation, and digital decision-making.

Keeping in mind the sensitivity of information and data collected in the IMPETUS Project's context, perhaps the **ethical evaluation capacity** represents the point of separation between a fully autonomous AI operation and human operator's takeover in the **decision-making process**. The noted switch of responsibility is likely to be enhanced by the *red-flag system* whereby the AI system alerts the human operator when the critical junction has been reached. The coding behind the noted system will allow designers (those who are designing the AI system) and deployers (those who are using AI system and/or offering services through that AI system, also commonly referred to as recipients, controllers, and processors) to delegate specific decision-making points to the AI system. Simultaneously, critical issues will remain reserved for human consideration, evaluation, and decision (compare with Asilomar, 2017). In any case, the coding should allow the human operator to freely interrupt the AI algorithm and evaluate its decision-making process (Floridi *et al.*, 2018).

In the IMPETUS Project's context, the above-noted process may be identified with instances where the AI system detects unwanted or suspicious behaviour on the part of known or unknown individuals. At that point, the human operator decides whether to proceed with a more comprehensive and invasive data collection and manipulation directed towards the noted subject(s). The human operator makes decisions concerning employing the AI system's empowered targeted/mass surveillance instruments (Feldstein, 2019) on an individual or group of individuals. The individual or a group in question are either a direct surveillance target or objects utilized to collect valuable information on the actual surveillance targets. The noted activities include various data collection capabilities: public or private CCTV systems, public or private smart devices (crowdsources surveillance (van Eck, 2018), including mobile tapping, tracking and collection functions of smart devices' applications, audio and visual recording (Milaj, van Eck, 2019), social network data mining, and similar), public or private sensors (such as body heat and other thermal equipment, movement, air/bio(chemical) and sound quality measurement, and others) and other technology (phone tapping and other) that collects data and information on their surroundings).

6.2.2 Supervision and oversight

Irrespective of whether the procedural points and checkpoints discussed above are later proven useful for the actual investigation, and regardless of whether both objects and subjects of investigation are later informed on such activities, the data collection and manipulation procedure must be documented. Proper documentation allows for proper *ad-hoc* and *post-hoc* supervision and oversight.

In terms of the purpose of supervision and oversight, the APPD Protocol (Art. 19) lists several required functions: investigation, intervention, approval of standards, approval of safeguards, decisions with regards to the violations, administrative sanctions, involvement in legal proceedings, reporting to competent judicial authorities, breach and violation investigation and reporting.

Whether or not a supervisory body and the oversight body should be the same bodies in charge of all instances of data processing is a matter that requires further examination, mainly keeping in mind the sensitive security and intelligence operations relevant for the IMPETUS Project's context.

6.2.3 Stakeholders

It is necessary to analyse how the various actors can be involved in security and intelligence data collection and manipulation. In the modern-day environment, such actors include a plethora of active and passive participants. The primary layer consists of public security agencies and institutions (i.e., police department, security apparatus, fire department, supranational bodies, etc.). The second layer consists of relevant public administration bodies (i.e., transportation authority, various city offices, and similar). A new, third layer has emerged in recent times, consisting of private entities contractually or non-contractually engaged directly or indirectly in security operations. The fourth layer represents ordinary citizens and legal persons involved either in autonomous or automatic data sharing/gathering.

Whereas the security services primarily use anonymous data to identify surveillance targets, private companies use anonymous data (Artificial Intelligence Committee, 2017) for commercial purposes. Individuals whose data is collected and analysed become objects rather than users. Such data may nor may not be re-identified. Still, questions are raised on whether private entities engaged in security and intelligence data collection and manipulation operations can avail of such data for other purposes. This issue deserves further consideration in the IMPETUS Project's context.

6.3 Critical requirements and principles

6.3.1 Ethics guidelines for trustworthy AI

The IMPETUS Project has determined that the development of an ethical framework must follow the Ethics Guidelines for Trustworthy AI (EGTAI, 2019), prepared by the High-Level Expert Group on Artificial Intelligence. The EU promulgates the EGTAI principles as the centre-piece of its AI Ethics strategy (Coordinated Plan, 2018).

The EGTAI determines that the notion of trustworthy artificial intelligence (AI) implies several components. The AI system must be **lawful** (compliance with regulations), **ethical** (adherence to values and principals) and **robust** (socio-technical adaptability). The AI system must also fulfil several specific requirements (human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental well-being, and accountability).

6.3.2 Critical requirements

This section primarily examines the **non-technical aspects of human agency and oversight, transparency, and accountability requirements**. The report analyses the noted requirements to the extent that they are relevant to the ethical issues concerning the security and intelligence operations involving data collection and manipulation.

The technical robustness and safety requirement are not analysed in this report. It primarily refers to the AI system's technical aspects concerning attack resilience, security, general safety, reliability, and fallback plan implementation (see Safe-DEED, 2020). However, one aspect of this requirement, **accuracy**, is of specific relevance for the IMPETUS Project context. It refers to the need for human operators to intervene and check the accuracy of individual decisions, predictions, or recommendations made by the AI system.

The privacy of data governance requirement is not analysed in this report. It primarily refers to the data privacy mechanisms (privacy of collected data, quality of collected data, data integrity, quality, and reliability of AI algorithms; see Safe-DEED, 2020). However, one aspect of this requirement, **access to data**, is of specific relevance for the IMPETUS Project context. It refers to the need to establish data access protocols.

The diversity, non-discrimination, and fairness requirements are not analysed in this report. It primarily refers to the issues of accessibility, universal design, and stakeholder participation. However, one aspect of this requirement, **avoidance of unfair bias**, is of specific relevance for the IMPETUS Project context. It refers to the need to have training and operational awareness concerning potential biases both within the AI algorithm and from the human operator perspective.

The societal and environmental well-being requirement is not analysed in this report. It primarily refers to the issues of sustainable and environmentally friendly AI and social impact. However, one aspect of this requirement, **the effect on society and democracy**, is of specific relevance for the IMPETUS Project context. It refers to the need to critically evaluate the ethical aspects and impact of data collection and manipulation in security and intelligence operations.

6.3.3 Fundamental principles

EGTAI states that ethical principles and values must be ever-present in all AI development and utilization stages. EGTAI highlights four fundamental principles: **respect for human autonomy, prevention of harm, fairness, and explicability**. The noted fundamental principles must be assessed in the IMPETUS Project's context. The following considerations are relevant for further analysis.

The respect for the human autonomy principle is particularly emphasized through the **need to secure human oversight over the AI system's operations**. The prevention of harm principle relates to the **secure and safe AI system's functioning** (elimination of malicious use or exploitation (Brundage, 2018)). Additionally, it underlines the importance of preventing negative impacts resulting from the **asymmetry of power and asymmetry of information**. The latter is especially relevant in connection to vulnerable groups (*inclusivity principle*). The fairness principle focuses on **eliminating bias and stigmatization** (prevention of unlawful and unfair use of data), stipulating the necessity of formulating clear procedural rules for human oversight of AI operations. The fairness principle additionally requires the **proportional application of measures**. The proportionality principle is reflected through the practice of undertaking **limited measures** to the extent necessary to achieve specific goals (scope limitation). The choice of measures undertaken should be guided by the desire to protect fundamental rights and ethical values (**qualitative/severity measures' limitation**). It also addresses people's potential right to redress the consequences of AI and human operators' activities. The latter relates to the principle of explicability that emphasizes the need for transparency of AI means and operations. EGTAI urges caution when employing AI systems, as such practices may have unwanted and unexpected consequences for society (i.e., the effect on distributive justice).

The noted principles must be further examined in the IMPETUS Project context, emphasizing the *public-to-citizen* relationship and security and intelligence operations' sensitivity and confidentiality. The ethical

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

framework should discern **to what extent are the noted principles applicable in the IMPETUS Project context**. EGTAI itself gives an example of "*predictive policing*", stating that the "*... surveillance activities* [may] *impinge on individual liberty and privacy*" (EGTAI, 2019:13), thus emphasizing a possible overlap or conflict between the relevant principles. EGTAI warns that an ethical framework cannot be constructed based on the principles alone but rather through an **evidence-based reflection**. The latter corresponds to the various data collection activities and pilot projects (to be) conducted through the IMPETUS Project. As per EGTAI, fundamental human rights are an inseparable component of a trustworthy and lawful AI. Therefore, when assessing big data, the AI system must incorporate safeguards to protect personal dignity and identity, considering people whose data is being captured and manipulated, not merely as objects but subjects with individual rights. EGTAI states that whenever there is a risk of an adverse effect on fundamental rights, each AI system operation must be preceded by a **fundamental rights' impact assessment**. In addition, EGTAI further notes that whenever an AI system affects fundamental rights, there ought to be an **independent audit system** in place (external auditors).

The freedom of the individual incorporates, among others, the right to be **protected from unjustified surveillance**, the right to private life, and the right to data privacy. EGTAI warns that mass or targeted surveillance, when conducted without a legitimate purpose and justification and by using disproportionate means, can lead to fundamental rights endangerment.

EGTAI stipulates that certain fundamental rights cannot be subjected to a trade-off and remain within the ethically acceptable norms. In cases where such measures are not ethically acceptable, the data collection and manipulation should not proceed. Where data collection and manipulation activities potentially infringe on private interests, such action must be identified, acknowledged, evaluated, and justified. All data collection and manipulation activities should be documented, and procedural and ethical rules on data collection and manipulation admissibility should be continuously reviewed and evaluated. Whereas EGTAI insists on dispute settlement mechanisms available to the third-party stakeholders (not only the compensation but all other means of rectification), it remains questionable and must be further examined to what extent such a mechanism can be implemented in the IMPETUS Project's context.

EGTAI suggests that **public sector data is preferred to personal data**. The latter indicates the extent to which the proportionality principle should be assessed in the IMPETUS Project context, having in mind both the available public and private technological means of collecting data.

Additionally, the level of human intervention in AI operations in the IMPETUS Project context must be further examined. Given the sensitive and often confidential security and intelligence operations, a human operator's role in the AI governance mechanism can be steered towards critical procedural instances when relevant decisions are made. Keeping in mind the scope and quantity of big data, the human-in-the-loop (HITL) approach, as EGTAI suggests, is unrealistic. It would be logistically impossible to have human operators remain responsible for each decision to collect and manipulate data. The human-on-the-loop (HOTL) suggests a human operator's access during the AI system design and monitoring capacity. Keeping in mind the nature of data collection and manipulation in the IMPETUS Project's context, it would appear that the **human-in-command (HIC) approach is the most suitable**. The HIC level of interaction allows the human operator's control over the AI system, including the choice of overriding or influencing (human discretion) a particular decision made by the AI, **full access, and oversight**. Keeping in mind the scope of collected data and analytical processes, it is inevitable that a large volume of data analysis will remain under AI's purview, resorting to *black-box post-hoc* investigation in cases of unwanted occurrences (Leslie, 2019). In the IMPETUS Project's context, it is vital to assess what sort of measures should be left for the human operator to decide upon, instigate or suspend.

The latter is closely connected to the explainability principle, requiring that the human operator can **understand and explain** (in plain language) the AI system's and human operator's **decision-making process** and understand **to what extent the AI algorithm influences both decision-making processes**. Whereas the former is a technical issue, the latter deserves further evaluation during the IMPETUS Project.

It should be noted that the above-mentioned principles are not necessarily followed by other HORIZON and similar projects dealing with the ethics of data collection and manipulation. As an example, the Safe-DEED project adopts the principles of autonomy, justice, beneficence, non-maleficence, and responsibility (Safe-DEED, 2020). Similarly, the European Ethical Charter on the Use of Artificial Intelligence in Judicial

Systems (published by the European Commission for the Efficiency of Justice (CEPEJ); CEPEJ, 2018) refers to respect for fundamental rights, non-discrimination, quality and security, fairness and transparency, and user control. The Alan Turing Institute has developed the FAST Track Principles set: fairness, accountability, sustainability, and transparency (Leslie, 2019). The noted and other principles (see: HECTOS, 2015; CUTLER, 2018; SHERPA, 2019; WITDOM, 2017; IEEE, 2019; Montreal, 2018; UN, 2018; OECD, 2019; G20, 2019; ACM, 2018; Berkman Klein, 2020; Also see: (Lorenz, 2020)) can, to a certain extent, be compared with that utilized by EGTAI. The IMPETUS ethical framework will assess the extent to which the EGTAI and other applicable principles are relevant for the IMPETUS Project's context.

PART II. REQUIREMENTS FOR PUBLIC SAFETY SOLUTIONS

7 Development of requirements

Based on the previous sections and results from D1.1, which describe the needs and challenges of public safety solutions, this section will describe the requirements supporting the development of the different results of the project (platform, tools, interface, frameworks). The requirements should describe especially:

- The objectives of the solution to be developed (needs to be addressed)
- Potential specificities of the partner cities
- Features or functionalities targeted
- Recommendation on the development process
- The origin of the requirements (e.g., DoA, WP1 task, other)

The figure below summarizes the scope, nature and sources of requirements in the project. The following sections will provide explanations for the different elements of the diagram.

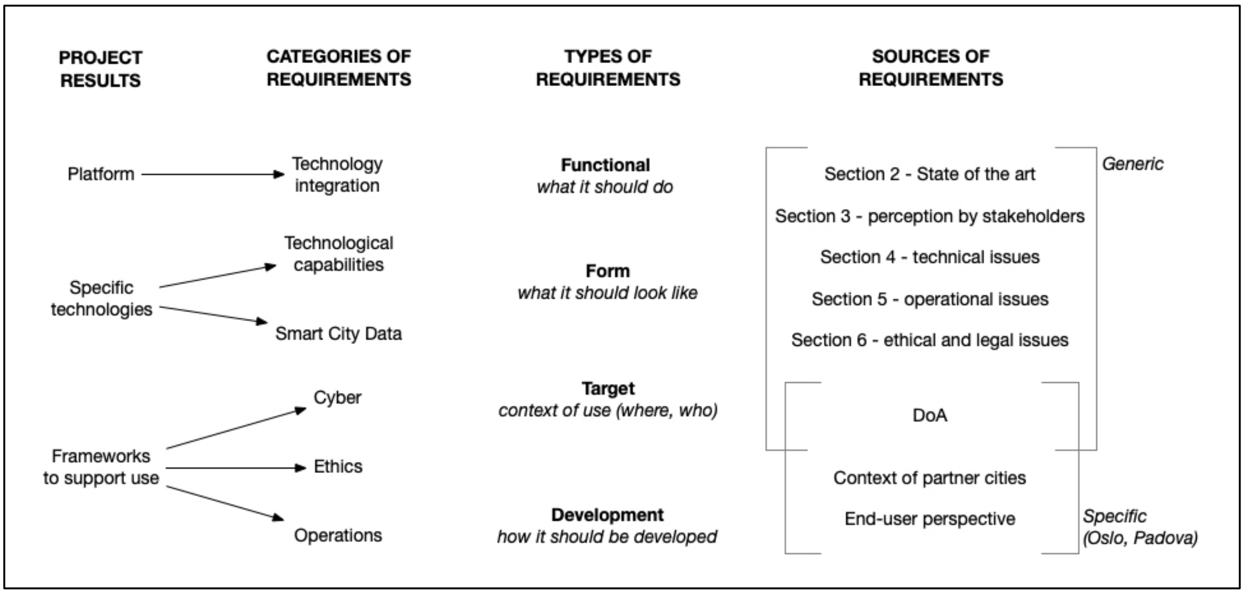
PROJECT RESULTS
CATEGORIES OF REQUIREMENTS
TYPES OF REQUIREMENTS
SOURCES OF REQUIREMENTS
Platform
Technology integration
Specific technologies
Technological capabilities
Smart City Data
Frameworks to support use
Cyber
Ethics
Operations
Functional
what it should do
Form
what it should look like
Target
context of use (where, who)
Development
how it should be developed
Section 2 - State of the art
Section 3 - perception by stakeholders
Section 4 - technical issues
Section 5 - operational issues
Section 6 - ethical and legal issues
DoA
Context of partner cities
End-user perspective
Generic
Specific (Oslo, Padova)

Figure 4. Scope, nature and sources of requirements

7.1 Development process

7.1.1 Core principles

We want to implement an iterative, agile-like process. This means it starts from proposing drafts, reviewing then revising them. The drafts do not have to be perfect, they serve to have a starting point/idea that will be improved through iterations. All these phases are important. In particular, the reviewing phase is crucial to go from basic ideas to directly usable requirements.

The requirements should be driven by user needs.

- There are generic requirements, which apply in principle to all smart cities, and there are specific requirements, which represent specific needs of our partner cities (they can overlap or not between them or with the generic requirements).
- A requirement should in most cases make one point only. If a statement makes two (or more) different points, it is usually better to split it.
- Requirements are not specifications. While precise, they should remain at a high-level of need description and not be tied to specific approaches or solutions.

7.1.2 Input to requirements

The requirements are motivated by different sources of information and different types of requirements are needed.

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

- Generic requirements
  - Part I (section 2-6) of D1.2 is the main source for generic requirements. It represents the background information about generic needs and challenges covering the different topics of the project (technical, operational, ethical/legal) in different subsections.
  - Another important source for generic requirements is the Excellence section (section 1) of the DoA.
  - The Description of Work (i.e. WPs and Tasks defined in the DoA, part A) is typically not a good source for the identification of new needs for requirements. However, the DoA provided a source for the basic requirements describing what we will do in the project.
- Specific requirements
  - The main source for specific requirements is D1.1 "Context of partner cities"[3] and other end-user (partner cities) perspectives obtained through detailed discussions with them in connection with production of this deliverable and wider project activities.

7.1.3 Process to draft, review and revise requirements

7.1.3.1 General organization

The elements below describe a collaborative process that takes advantage of the consortium's diversity. The requirements development process was supported by internal guidance documents as well as by weekly status meetings, complemented as needed by punctual meetings and interactions. All partners were involved, but with different roles:

- **RE (Research)**
  - Partners involved in Part I of D1.2 (about "Background")
  - draft generic requirements
  - coordinate with colleagues and/or other RE partners to improve the draft before considering it ready for review
  - revise requirements based on PC and TP feedback
- **PC (Partner Cities)**
  - Partner cities, with the help of exploitation leaders:
  - review the draft requirements
  - comment on their clarity from an end-user standpoint
  - assess their importance
  - identify whether additional, more specific requirements are needed for the point addressed by a requirement.
- **SP (Solution Providers)**
  - Partners providing elements of the IMPETUS "solution" i.e., the technologies that we will create/refine *and* supporting materials such as Practitioner's Guides (aka "frameworks")
  - review the draft requirements
  - comment on their clarity from a solution provider standpoint
  - assess their feasibility
  - provide information about the needs or constraints for their fulfilment

In the list above, we have assigned just one role to each partner involved. The main principles behind such organisation of tasks are:

1. The group of partner(s) who review a particular requirement cannot overlap with the ones who drafted it.
2. No partner, regardless of role, is excluded from proposing and drafting a requirement if they perceive it to be important for the overall success of the project. Thus: the indications above about who drafts what kind of requirements are general expectations, not absolute rules.

[3] D1.1 has "EU RESTRICTED" status; for details of its relationship with this deliverable please refer to section 1.4.

7.1.3.2 *Importance of the review and revision process*

The process proposed and implemented aimed at being agile and iterative. Following this approach, the initial emphasis was put on producing draft requirements based on the identification of needs and associated insights. The objective was not to produce perfect requirements from the beginning, but rather to quickly capture and propose essential ideas. Going from initial ideas to well-stated and approved requirements relied on the involvement of reviewers, the review process feeding a cycle of revisions to collaboratively improve the content developed. Typically, each requirement was reviewed by more than one reviewer.

The first part of the review process focuses on the clarity of the requirement statement and associated information. Using dedicated text fields in the requirements structure (see section 7.2 below), reviewers and authors exchanged questions, suggestions and clarifications. When review comments were clear, authors were expected to indicate whether the review points have been addressed, and provide potential comments or questions to support discussion with the reviewer(s). When review comments were not clear, or in case two reviews provided did not agree, requirements authors were instructed to get in touch with the reviewer(s) to work collaboratively on revising the requirement.

The second part (still on-going) focuses on the importance and feasibility assessments, from cities and solutions providers, respectively. When a draft requirement is considered accepted (has gone through some revisions), cities and solutions provider(s) are contacted to provide further review and conduct Importance and Feasibility assessment.

7.1.4 Challenges in requirements development

7.1.4.1 *Homogenisation of content*

Due to the wide scope and multi-disciplinary nature of the project, the development process frequently led to heterogeneous results. Heterogeneity in the statements corresponded especially to differences in language and level of specificity. A sub-team was established late March to collaboratively review around 80 drafted requirements and make progress on homogenising their content. Ten partners shared the list of requirements and reviewed a dozen requirements, creating overlap between reviewers. Results of the review process were captured in a shared document and discussed as a team to make propositions for improvement. Among the main propositions were:

1. the quasi-systematic use of *should* statements combined with the Importance field, rather than the MoSCoW (must, should, could, won't) prioritization language used initially
2. a harmonization in terminology (e.g., platform/system, technology/solution/tool)
3. the emphasis on the need to make more obvious what requirements apply to

7.1.4.2 *Remaining uncertainty:*

During the process, partners noted that they found difficult to make progress on producing clear requirements while other efforts in parallel in the project aimed at better defining the project results and ambitions. Requirements' development, however, offered an opportunity to define what we should accomplish – so constituted a process where uncertainty was addressed to some degree.

7.2 Requirements format and content

7.2.1 Format

The requirements are captured in a structured document (customised Sharepoint List) shared on the project's restricted access file-sharing and cooperation platform. A structure was developed to describe two aspects of each requirement:

- Its <u>content</u>, starting with the same fields as currently used in the Excel sheet. Additional fields might be added when gaps are identified.
- Its <u>management information</u>, to better identify authors and contributors, comments, revisions, status, etc.

The following table provides the description of each field in the List of Requirements:

Table 8. Format of requirements in Sharepoint List

Field Name	Meaning of the field	Format / Possible values
ID	An automatically generated value that uniquely identifies the requirement. The value of the field has no semantic significance.	A positive integer.
Requirement	A concise statement of the essence of the requirement.	Free text, not exceeding 255 characters.
Rationale	Description of the motivation behind the requirement.	Free text.
Category	Provides a broad categorization of requirements based on the type of support to which they relate.	"Choice" field (one value), with the possible values: • **Ethics**: Dealing with ethical, legal and data privacy issues • **Cyber:** Preventing, detecting and dealing with cyber security risks • **Operations:** Dealing with potential changes in working processes and/or the impact of such changes • **Smart City Data:** Dealing with issues of Big Data, data management and processing • **Technological capabilities**: Support needed from specific technological solutions. • **Technology integration**: Support needed to allow technological solutions to work together and with existing technical systems.
Type	The nature of the requirement.	"Choice" field (one value). The numbers at the start of the field values have no particular meaning, they simply facilitate the sorting of requirements: • **10 Functional**: What behavior / features / functions / information are needed. • **20 Form**: How (1): needs related to how relevant project result(s) should "look like" e.g. format, how accessed etc. • **30 Targeted use**: Who needs support and in what context. • **40 Development**: How(2): Process to be used to develop relevant project result(s). • **50 Evaluation**: How(3): Process and criteria to be used to evaluate relevant project result(s).
Author_	The name of the partner/person who lead the development of the requirement.	Short name of partner/name of individual

Field Name	Meaning of the field	Format / Possible values
Reviewer	The name of the person in charge of coordinating the review of the requirement, to decide about whether it will be "approved" or not.	Short name of partner/name of individual
Importance	An assessment by primary stakeholders (i.e., Partner Cities) of how important it is that the requirement be fulfilled.	"Choice" field (one value): • **01 Deal breaker**: Without this, the relevant part of the IMPETUS solution is not fit for purpose. • **02 Required**: We definitely want this, but it is not a deal-breaker for the overall solution. • **03 Nice-to-have**: We can for sure get by without this. But if it is easy/fast to implement – please do it.
Comments importance	Comments on the "Importance" field e.g., providing extra details justifying why the requirement is a "deal breaker".	Free text. • Each comment should have a blank line after it, to separate it from the comment that comes next. • Each comment should start with the name of its author + the date. • Comments should be sorted so that the latest comment comes first.
Feasibility	An assessment by the partners who would be responsible for fulfilling the requirement of how easy it would be to do so.	"Choice" field (one value): • **01 Difficult**: It would be very difficult (maybe impossible) or very expensive to implement this. • **02 Doable**: It is possible to implement this, and the effort required is within the scope of available resources. • **03 Easy**: This can be implemented quickly and without significant use of resources.
Comments feasibility	Comments on the "Feasibility" field, e.g., providing extra details justifying why the requirement is considered "Difficult".	Free text. But see notes on field "Comments importance" for some simple formatting conventions.
Source	Short reference to any document(s) or other external source(s) providing extra information about / rationale for the requirement.	Free text. Possible examples: part of a deliverable, DoA, policy document from a city, …

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

Field Name	Meaning of the field	Format / Possible values
Status	Indicates the stage reached in the workflow used for handling requirements. This covers both the process of deciding whether a requirement should be "approved" (i.e., the whole team agrees that the requirement should be fulfilled) and the process of tracking implementation of approved requirements.	"Choice" field (one value). The numbers at the start of the field values are primarily used for sorting of requirements. However. all states numbered 50 or more are terminal states, i.e., once the state has been reached the requirement is no longer active, it is retained for archival/reference purposes only. • **10 Draft**: A new requirement has been drafted (normally by one of the "RE" partners for generic requirements or a PC partner for specific requirements). The "Importance" and "Feasibility" fields would probably not be filled in at this stage. • **20 Under review**: The requirement is being reviewed (by all partners to whom it is relevant). The "Importance" and "Feasibility" fields would typically be filled at this stage, together with the associated "_comments" fields. • **25 Under revision**: The requirement is being updated in the light of comments and feedback from the "Under review" stage. • **30 Approved**: The team have reached agreement that this requirement should be implemented but work on doing so has not yet started. • **40 Being implemented**: Work is in progress to implement the requirement. • **50 Implemented**: The requirement has been implemented to the satisfaction of the stakeholders. • **60 Split**: It was decided that the requirement is too big/complex, so it has been split into several simpler requirements. The simpler requirements will be followed up as new requirements, this one is archived. • **61 Merged**: It was decided that the requirement is so closely linked to another requirement, that it is best to merge this requirement into the other one. This requirement is retained in the list for archival/traceability purposes but is no longer active; the other requirement into which this one was merged remains active. • **70 Dropped**: The stakeholders who originally proposed the requirement and/or other affected stakeholders have all decided that the requirement is no longer relevant/important/needed, or consider that it has been superseded by another requirement. The requirement is retained in the list for archival/traceability purposes but is no longer active. • **71 Rejected**: The project team has decided that we will not plan to implement this requirement. This might be because it is regarded as not sufficiently important/relevant, or too difficult/costly to implement – or for any other reason that they might decide. The requirement is retained in the list for archival/traceability purposes but is no longer active.

Field Name	Meaning of the field	Format / Possible values
Dependencies	Notes indicating any direct or indirect dependencies on other requirements (referred to using their ID).	Free text. Examples of possible dependencies: • The way that this requirement is implemented could be influenced by the way in which another requirement is implemented. • This requirement becomes more or less important/relevant depending on the how/whether other(s) are implemented. • This requirement has a "sub-requirement" relationship with another. • There is no hard dependency, but there is some kind of relationship that should be kept in mind.
Comments approval	*Used before a requirement has been approved:* Comments that contribute to general discussions about the requirement, in particular whether it should be "approved" or not. Complements the "Comments importance" and "Comments feasiblity" fields.	Free text. But see notes on field "Comments importance" for some simple formatting conventions.
Comments implementation	*Used AFTER a requirement has been approved:* Comments providing information about the status of implementation of a requirement, including discussions about how its status should be updated (e.g., do the partners agree that implementation is good enough to change state to "50 Implemented").	Free text. But see notes on field "Comments importance" for some simple formatting conventions.

7.2.2 Fully detailed examples of requirements

In this sub-section, we present 2 examples of requirements with the information described above. The layout presented is very similar to what appears on-screen when using the requirements list on SharePoint. An objective of such layout is to better identify the types of information expected. *The reason for providing these examples is simply to give some insight into the process and working procedures used in developing the requirements.*

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

BASIC INFORMATION		
ID	**Requirement**	
33	The IMPETUS platform/tools should provide appropriate transparency when it provides insight into the information sources and the calculations that contribute to the recommendations and predictions provided to a user.	
Author	**Reviewer(s)**	**Status**
Thales		25 Under revision
Type	**Category**	**Sub-category**
20 Form	Technology integration	
INFORMATION ABOUT REQUIREMENT		
Rationale		
Observability provides transparency into what the IMPETUS platform/tools is doing relative to users' task progress within the City Command & Control context. Observability supports shared understanding of the problem to be solved and progress toward goals. The IMPETUS platform/tools are considered observable when it provides the right level of information, so the user understands its recommendations and predictions.		
Source		**Dependencies**
WP1 (human machine teaming), WP7 (user validation)		
ASSESSMENT		
Importance	**Comments importance**	
02 Required	CPAD important	
Feasibility	**Comments feasibility**	
REVISION		
Approval level	**Comments approval**	
	26/02 SINTEF - Needs rephrasing, "what it is thinking" is unclear. What matters is that the user knows what the platform/tools are doing and why (e.g., understand what is generating a message). - This is a "Form" requirement. But "observability", "predictability", etc. should be used to define criteria for evaluation 02/02 THA Rephrased 23/03 CPAD please write an example to clarify the meaning of "observability" to be sure of being on the same page	
Implementation level	**Comments implementation**	

BASIC INFORMATION		
ID	**Requirement**	
58	The Access Control methodology and the ingestion process must use standard interfaces.	
Author	**Reviewer(s)**	**Status**
CINI-UMIL		25 Under revision
Type	**Category**	**Sub-category**
40 Development	Smart City Data	
INFORMATION ABOUT REQUIREMENT		
Rationale		
Support the communication with other parties. Access control methodology and ingestion process can work at different points including the overall platform and tools. Each specific tool could have its own access control methodology and ingestion process. Simplified Description: Traditional requirement to ease the integration between different components using standard APIs		
Source		**Dependencies**
DoA		
ASSESSMENT		
Importance	**Comments importance**	
02 Required	CPAD important: the use of API is strongly "advocated"	
Feasibility	**Comments feasibility**	
REVISION		
Approval level	**Comments approval**	
	26/02 SINTEF “expose” is unclear. avoid reference to solutions provided (access control or ingestion engines), but rather mention generic capability 21/05 SINTEF - changed to must since mentioned in DoA	
Implementation level	**Comments implementation**	

8 Overview of requirements for the development and implementation of public safety technology

The requirements are directly related to the scope and objectives of project IMPETUS: the main ambitions of the project are related to (1) integrating mostly mature technologies for public safety in a smart city environment, and (2) producing accompanying guidance and tools to address the operational, legal and ethical, as well as cyber security aspects of the use of such capabilities. The requirements presented in this document therefore reflect these primary concerns.

In this section, we provide a full list of all active requirements but showing only three key fields. To facilitate readability, the list is organized here by category (i.e., according to the project results they primarily address), then by requirement type. If you are interested to see details of other fields, please refer to Appendix B, which shows all requirements sorted by the integer "ID" number (shown in the right column in the table below).

8.1 Requirements for the Public safety Platform

Type	Requirement	ID
10 Functional	The public safety platform must integrate different capabilities for public safety	52
10 Functional	The IMPETUS platform should be a modular platform where the individual tools can be added or removed without negating the functionality of the platform as a whole.	49
10 Functional	The Impetus modules must be easy to integrate with other tools if needed	95
10 Functional	The IMPETUS platform must remain a standalone platform but should be able to interact with existing devices and platforms in the cities.	97
10 Functional	The Impetus platform inputs-outputs should be customised according to the specificities of the cities (not only the pilot ones)	90
10 Functional	The platform should provide a secure access to the specific tools from the integrated view.	53
10 Functional	The IMPETUS platform/tools should provide the choice betwen multiple levels of automation to best support operators in recognizing and adapting to unexpected situations.	48
10 Functional	The IMPETUS platform should allow for sharing of information to users from organisations which are not part of the IMPETUS operating environment through data exports, embedded views or guest access according to operational needs.	28
10 Functional	Platform owners and operators should be able to filter, aggregate, compile (specific) data into formats which can be easily forwarded to other users from organisations which are not part of the IMPETUS operating environment.	51
10 Functional	The platform should allow for logging of "false alarms".	55
20 Form	The IMPETUS platform should be easy to use for a variety of final users.	41
20 Form	The IMPETUS platform should be able to provide different views from the available data according to the users' needs	35
20 Form	The platform interface should support different forms of interaction depending on situation and user profile.	22
20 Form	The platform interface should allow end-users to configure which tools they want to use at a given time, depending on their operational needs.	43
20 Form	To ensure synchronisation between security actors, the same interface visualizations and alerts should be provided to different SOCs.	27
20 Form	IMPETUS platform should have 2 different interfaces, one for physical events SOC operators, another for cybersecurity SOC operators.	42

Type	Requirement	ID
20 Form	When something suspicious or alarming is detected, the platform interface should provide an alert that effectively grabs the attention of the operators.	44
20 Form	The IMPETUS platform should provide alerts for different operators within the same organisation or emergency service.	98
20 Form	The IMPETUS platform should provide alerts for different operators across different organisations.	99
20 Form	The IMPETUS platform/tools should provide appropriate transparency when it provides insight into the information sources and the calculations that contribute to the recommendations and predictions provided to a user.	33
20 Form	The IMPETUS platform/tools should provide transparency of future intentions, states, and activities, as well as a projection of what the future situation will be if current trajectories are continued.	34
20 Form	The IMPETUS platform/tools should update their assumptions to support the user.	40
20 Form	The IMPETUS platform/tools should (proactively) direct the attention of users to critical problem features, cues, indications, and warnings when information become relevant.	36
20 Form	The IMPETUS platform/tools should help problem solving by suggesting actions to consider and offering alternative suggestions.	37
20 Form	The IMPETUS platform/tools should be clear about it's trustworthiness/confidence level so users can determine how much and when to trust it.	39
20 Form	The IMPETUS platform/tools should be able to let the user control (stop or override) its processes.	38
20 Form	The user interface (including graphical elements) should be available in multiple languages, including the language(s) preferred locally by end-users.	45
30 Targeted use	The platform must be compatible with existing infrastructures for data collection adopted by the city	32
30 Targeted use	The development of the platform and the specific tools should consider the connection of simultaneous users	30
30 Targeted use	The platform should allow for logging and saving of findings in such a manner that it can be used as legal evidence in court.	103
30 Targeted use	The IMPETUS platform should be intended to always be in operation	86
30 Targeted use	The public safety platform should be easily maintained by the technical staff of the city	31
30 Targeted use	The IMPETUS platform should allow the connection of simoultaneous users.	54
30 Targeted use	The IMPETUS platform should be able to provide access rights for end users based on roles, responsibilities and operational needs.	50
30 Targeted use	Smart cites should have immediate cross organizational communications channels that are known, interoperable and of suffient bandwidth to account for surge capacity.	56
30 Targeted use	The platform administrator should be able to integrate tools and to configure the interface (e.g, visualizations).	89
30 Targeted use	The Impetus platform should not be modified by the operative end-users	87
30 Targeted use	The Impetus platform should be supplemented with a detailed user manual (usage and ordinary maintenance).	87
30 Targeted use	The platform should support operations during all phases of the intelligence cycle.	74
40 Development	The project should implement a progressive testing and validation of the platform.	117
40 Development	The IMPETUS platform development should implement a user-centred approach to address user needs and input.	116
40 Development	The IMPETUS platform should be mainly validated through pilots conducted in the partner cities.	118

Type	Requirement	ID
40 Development	The IMPETUS platform should adapt a common terminology and symbology	24

8.2 Requirements for the specific Public safety Capabilities

Type	Requirement	ID
10 Functional	The IMPETUS project must advance the design of specific technological solutions to improve the management of public safety events in the smart city, from threat detection to the response to physical and/or cyber events.	114
10 Functional	The IMPETUS platform should include detection and alerts of suspicious content from social media.	88
10 Functional	The IMPETUS tools should have analysis functions that enable the operators to filter and narrow down the information that is collected according to intelligence needs.	76
10 Functional	In the case of security events, the Impetus platform should provide the possibility to alert the population of an emergency situation (e.g., via text messaging or other channel).	92
10 Functional	The IMPETUS platform should be open to receive input from city officials/emergency personnel to integrate the information received by sensors/data	96
30 Targeted use	The platform tools involving social media, dark web and cyber threat intelligence should allow for targeted intelligence collection.	75
30 Targeted use	The implementation of edge devices should conform to their recommended range of utilisation and avoid increasing vulnerabilities.	71
30 Targeted use	Results from AI should always be monitored by humans before leading to action.	59
40 Development	The project should focus on using and improving proven technologies with the aim of combining them into an integrated solution.	112
40 Development	Relevant sensor data should be provided by the smart cities to properly train AI/ML-based tools.	68
40 Development	Sensors should be made available (potentially installed) in the smart cities to support the use of the individual tools.	70
40 Development	The cyber integrity of tools and their components should be ensured before their integration in the platform.	73
40 Development	Alerts from tools should be tested and developed in accordance with systems and protocols in place in the smart cities.	69
40 Development	Design and development of the platform technologies should take into account human factors and capabilities.	84

8.3 Requirements for the management and processing of Smart City data

Type	Requirement	ID
10 Functional	The IMPETUS project must develop approaches and methodologies for large-scale data analytics and visualization, as well as implement access control requirements to ensure the security of the data.	115
10 Functional	The platform should support data and control flow integration.	78
10 Functional	An Access Control methodology should handle access rights and data control.	1
10 Functional	The Access Control methodology should support sanitization policies that are enforced at ingestion time before an access to data is granted.	3
10 Functional	The ingestion process should support ingestion of structured and unstructured data.	61

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

Type	Requirement	ID
10 Functional	The Ingestion process must support standard ingestion workflows on data measured and collected by the pilot cities.	63
10 Functional	Data analytics should be executed on ingested data.	62
20 Form	The IMPETUS platform should support users in creating personalized aggregated data and diagrams to perform specific analyses.	101
20 Form	The IMPETUS platform should provide aggregated data and diagrams to allow for strategic monitoring and planning.	100
20 Form	The change detector should raise an alert when sensor data do not follow an expected behavior, according to historical data for any variable under observation	46
20 Form	The event classifier should raise an alert when sensor data represents a previously defined class of threat	47
30 Targeted use	The platform operators should manage Access Control policies.	60
40 Development	The Access Control methodology and the ingestion process must use standard interfaces.	58
40 Development	The change detector and event classifier stages (training/working) should be controlled remotely	29

8.4 Requirements for the Cyber security Framework

Type	Requirement	ID
10 Functional	The IMPETUS project must develop a cybersecurity framework to support Smart Cities in addressing cyber security issues associated with technology for safety.	105
10 Functional	The cyber security framework should inlcude tools enabling smart city operators to simulate, validate and remediate cyber-attack paths to critical assets.	107
10 Functional	The cyber security framework should include a security awareness training.	106
10 Functional	The IMPETUS Cybersecurity framework should provide a data collection system	5
10 Functional	The data collection system should collect system configuration information	4
10 Functional	The data collection system should provide a standard based interface for data collection from data sources forming part of the monitored system	2
10 Functional	The IMPETUS Cybersecurity framework must contain an information correlation engine	6
10 Functional	The information correlation engine must identify common information elements across the multi-source information received by the data collection system	7
10 Functional	The correlation results should be stored securely in an encrypted form	8
10 Functional	The IMPETUS Cybersecurity framework should provide a response system, to handle both proactive and reactive mitigation of threats and attacks	9
10 Functional	Mitigation actions proposed by the response system to handle threats and attacks should minimize the impact of such threats and attacks against the system	10
10 Functional	Mitigation actions proposed by the response system to handle threats and attacks should minimize collateral damages of actions themselves	11
10 Functional	The response system should benefit from the use of anomaly detection, in order to derive new attack patterns	12
10 Functional	The IMPETUS platform must be protected from outside intruders.	93
40 Development	The cyber security awareness training should be based on the existing open source Security Culture Framework.	108

8.5 Requirements for the Ethical and legal Framework

Type	Requirement	ID
10 Functional	The IMPETUS project should develop an ethical framework to support Smart Cities in addressing ethical and legal issues associated with technology for safety.	111
10 Functional	The ethical guidelines should assess the risks to fundamental data rights and data privacy.	18
10 Functional	The ethical framework should address issues such as artificial intelligence biases	109
10 Functional	The IMPETUS platform should have well defined user roles to guarantee access to personal data only to authorised authorities and individuals.	79
30 Targeted use	The Ethical Framework should be developed as a tool for decision-makers, actors of the city investing in and using security and smart city solutions.	110
30 Targeted use	Smart cities should inform citizens on risks of adopting integrated platforms and technologies	19
40 Development	The development of an ethical guidelines must follow the Ethics Guidelines for Trustworthy AI	13
40 Development	The ethical guidelines should consider the role of State, its obligation toward use of all available means (including technology) to protect its citizens, and its obligation to protect citizens personal data and privacy.	16
40 Development	The ethical guidelines should consider certain relevant aspects concerning the collection of data on one side, and privacy and personal data protection on the other	15
40 Development	The ethical guidelines should thoroughly examine the ethical issues connected to the deployers category.	14
40 Development	Smart cites must develop a legal taxonomy for relevant data sets and flow down the requirements to all partners	17

8.6 Requirements for the Operational Framework

Type	Requirement	ID
10 Functional	The IMPETUS project must develop new concepts of operation and implementation guidelines to support the use of new technological capabilities in operations.	104
10 Functional	The new concepts of operations should address degraded modes during which the public safety platform or tools are not fully functional.	113
10 Functional	Operations supported by the platform should comply with the national/international (if applicable) security frameworks, including legal and cyber related frameworks.	25
10 Functional	Roles, tasks and responsibilities in the decision-making process should be defined clearly in the new concepts of operation.	82
10 Functional	Division of responsibilities should be defined clearly relative to the use of tools in the platform, including who is using which tool(s) based on authority and skillset.	83
10 Functional	Smart cities should develop a methodology and process to monitor social media and open news sources.	26
10 Functional	Smart cites should develop a methodology to utilize CCTV sources and ensure their effective use, including related to technical and social aspects	57
10 Functional	Training plans for all relevant security actors should be created to address the concepts of operation with the public safety platform	23
10 Functional	Training plans should be created to prepare operators and first responders for using the platform during complex and stressful scenarios.	81
30 Targeted use	The platform should allow for efficient and coordinated information sharing between SOC operators and responders in the field in a purposeful format in order to increase situational awareness for first responders.	102
30 Targeted use	Information generated from the IMPETUS platform should be accessible from different emergency services and operational stations.	94
30 Targeted use	Performing or receiving threat assessments and mapping of threat actors and targets should be part of the routine for the operators of the platform.	80

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

Type	Requirement	ID
30 Targeted use	The platform should allow for efficient information sharing between operators from different intelligence disciplines.	77
40 Development	The security actors should lead the definition of new concepts of operation taking advantage of new technological capabilities.	20
40 Development	The definition of new concepts of operation should identify and involve all relevant actors of security, covering daily activities as well as rare events.	21

9 Conclusions and next steps

9.1 Challenges and limitations in requirements development

The requirements' development process was defined, tested and adjusted during the first months of the project before settling on a form that supported collaborative work. The process was further complicated by the highly multi-disciplinary nature of the project and consortium, as well as by the almost exclusively virtual collaboration. Indeed, due to the pandemic, the absence of dedicated physical meeting made difficult the initial building of common ground on objectives and approach. This led to difficulties in producing more homogenous content early in the process, for instance in the terminology or in the level of specificity of the requirements.

A balance needed to be found between Requirements and Specifications, especially for work packages producing technical results. The choice was made that requirement should be relatively abstract and that the WPs responsible to address them should describe in specifications how they will be implemented – but this distinction proved challenging in practice. The requirements described in this document are the result of this effort to be both abstract and specific enough.

As a result of the previous point, it was also decided not to include an "Evaluation" category for requirements. The "evaluation" category of requirements was initially envisioned in order to capture how the fulfilment of requirements was to be evaluated and therefore to serve as a basis to validation work in WP7. In the end we decided that it is more effective for requirements defined here to capture high-level principles (e.g., human-factors interface principles) and leave it to WP7 to identify in more detail how best to evaluate these in practice.

9.2 Maturity of the requirements presented

The list of requirements is a standalone document that will be improved (completed, refined, clarified) during the project, as more information and deeper understanding becomes available about needs or constraints. This deliverable therefore provides a snapshot of the requirements that will be produced in the project.

To support development and evaluation of project results, requirements needed to be sufficiently complete and mature as early as possible. Our objective was to reach 80% completion (coverage and maturity) on release of this deliverable (May 2021). "80%" is a rough estimate that cannot be measured precisely; it represents significant advancement while acknowledging that we have reached the final version of requirements.

The list of requirements here presented have all gone through several cycles of review and revision, and we are satisfied that all key areas of coverage are included. We therefore consider that we have reached the coverage and maturity objective as defined.

9.3 Evolution of the requirements

A significant change in the initial vision of the development of requirements is the consideration of the list of requirements as a living document. As a result, evolutions are expected beyond the content presented in this document:

- First of all, the current priority is to finalize the assessment of Importance and Feasibility by partner cities and solution providers, respectively.
- Next steps aim to transition from the development of requirements to their implementation. This includes prioritizing the existing requirements, based especially on the importance and feasibility assessments. We also plan to organize a prioritization with external stakeholders, involving COSSEC members especially.
- Finally, regular efforts will be made during the life of the project to further improve content (e.g., clarity) and address potential gaps.

10 References

For convenience purposes, due to the large amount of references in the document, the references are presented below divided by section (all from "Part I").

10.1 State of the art: technological capabilities currently implemented in smart cities

[1] Yeh, H., 2017. The effects of successful ICT-based smart city services: From citizens' perspectives. *Government Information Quarterly*, 34(3), 556-565.

[2] Ismagilova, E., Hughes, L., Rana, N.P., Dwivedi, Y.K., 2020. Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Information Systems Frontiers.

[3] Albino, V., Berardi, U., Dangelico, R.M., 2015. Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of urban technology*, 22(1), 3-21.

[4] Deakin, M., 2013. From intelligent to smart cities. In Deakin, Mark (ed.). *Smart Cities: Governing, Modelling and Analysing the Transition.* Taylor and Francis, p. 15.

[5] Forbes (2019). These are the smartiest cities in the world for 2019. Accessed on 24.11.2020.

[6] Singh, P., Dwivedi, Y.K., Kahlon, K.S., Sawhney, R.S., Alalwan, A.A., Rana, N.P., 2019. Smart monitoring and controlling of government policies using social media and cloud computing. *Information Systems Frontiers*, 1-23.

[7] Moir, E., Moonem, T., Clark, G., 2014. What are future cities? Origins, meaning and uses. Compiled by the Business of Cities for the Foresight Future of Cities Project and Future Cities Catapult. Government Office of Science, U.K.

[8] Eremia, M., Toma, L., Sanduleac, M., 2017. The Smart City Concept in the 21st Century. *Procedia Engineering*, 181, 12-19.

[9] Hodgkinson, S., 2011. Is Your city smart enough? *Digitally enabled cities and societies will enhance economic, social, and environmental sustainability in the urban century.*

[10] Hsi-Peng Lu, Chiao-Shan Chen, Hueiju Yu., 2019. Technology roadmap for building a smart city: An exploring study on methodology. Future Gener. Comput. Syst. 97: 727-742.

[11] Kafi, M.A., et al., 2013. A study of wireless sensor networks for urban traffic monitoring: Applications and architectures. Procedia Computer Science, 19, pp. 617-626.

[12] Muttillo, M., Muttillo, V., De Rubeis, T., 2020. Towards the Design of Microcontroller Based Embedded Sensory systems with a Five-Parameter Single Diode Estimation Method for Photovoltaic Panels (2020) 2020 IEEE International Workshop on Metrology for Industry 4.0 and IoT, MetroInd 4.0 and IoT 2020 - Proceedings, art. no. 9138311, pp. 197-201.

[13] Qusay I. Sarhan, 2020. Systematic Survey on Smart Home Safety and Security Systems Using the Arduino Platform IEEE Access, 8, 128362–128384.

[14] Mahdavinejad, M.S., et al., 2018. Machine learning for internet of things data analysis: a survey. Digital Communications and Networks, 4 (3), pp. 161-175.

[15] M. Dittenbach, D. Merkl , A. Rauber, The growing hierarchical self-organizing map, in: Proceedings of the IJCNN, IEEE, 20 0 0, p. 6015.

[16] Ameya Malondkar et al., 2019. Spark-GHSOM: Growing Hierarchical Self-Organizing Map for large scale mixed attribute datasets. Inf. Sci. 496: 572-591.

[17] Meng, X., et al., 2016. MLlib: Machine learning in Apache Spark, Journal of Machine Learning Research, 17.

[18] Corizzo, R., et al., 2019. DENCAST: distributed density-based clustering for multi-target regression, Journal of Big Data, 6 (1), art. no. 43.

[19] International Organization for Standardization, 2018. ISO 37120:2018. Sustainable cities and communities. Indicators for city services and quality of life.

[20] Shah, J., Kothari, J., Doshi, N., 2019. A Survey of Smart City infrastructure via Case study on New York. EUSPN/ICTH 2019: 702-705.

[21] Yasir Mehmood et al., 2017. Internet-of-Things-Based Smart Cities: Recent Advances and Challenges. IEEE Commun. Mag. 55(9): 16-24.

[22] Rodulfo, R., 2020. Smart City Case Study: City of Coral Gables Leverages the Internet of Things to Improve Quality of Life IEEE Internet Things Mag., 3(2), 74–81.

[23] https://smartcities-infosystem.eu/sites-projects/projects (last accessed: dec, 2020)

[24] https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart_cities_en (last accessed: dec, 2020)

[25] El Baz, D., Bourgeois, J., 2015. Smart cities in Europe and the alma logistics project. ZTE Communications, 13(4), 10-15.

[26] https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET%282014%29507480_EN.pdf

[27] https://media.iese.edu/research/pdfs/ST-0542-E.pdf

[28] https://international.kk.dk/sites/international.kk.dk/files/the_capital_of_sustainable_development_sustainable_development_goals_2018.pdf

[29] https://trello.com/b/CIoKi2mP/smarter-london-together-report-card (last accessed: dec, 2020)

[30] https://www.gsma.com/iot//wp-content/uploads/2016/10/GSMA-Crowd-management-case-study-web.pdf

[31] https://safecities.economist.com/wp-content/uploads/2019/08/safe-cities-index-eng-web.pdf

[32] https://safecities.economist.com/wp-content/uploads/2019/08/Aug-5-ENG-NEC-Safe-Cities-2019-270x210-19-screen.pdf

[33] https://statetechmagazine.com/article/2020/01/power-smart-street-lighting-smart-cities-perfcon (last accessed: dec, 2020)

[34] https://india.smartcitiescouncil.com/article/emergency-call-boxes-pas-environmental-sensors-many-more-pune (last accessed: dec, 2020)

[35] https://smartcitiescouncil.com/article/your-website-and-social-media-prepared-emergency (last accessed: dec, 2020)

[36] https://archive.triblive.com/local/pittsburgh-allegheny/pittsburgh-expanding-system-of-smart-traffic-lights-to-ease-congestion/ (last accessed: dec, 2020)

[37] https://connectedworld.com/connected-urban-transport-solution-helps-dallas-work-smarter/ (last accessed: dec, 2020)

[38] https://www.opcw.org/work/what-chemical-weapon

[39] https://www.ncbi.nlm.nih.gov/books/NBK230682/

[40] Biswas et al., 2016. Securing smart cities using blockchain technology. 18th international conference on high performance computing and communications, pages 1392-1393

[41] Ivanov et al. Automatic security management of smart infrastructures using attack graph and risk analysis, 4th World Conference on Smart Trends in Systems, Security and Sustainability, pages 295–300, 2020.

[42] Botello et al., 2020. BlockSIEM: Protecting smart city services through a blockchain-based and distributed SIEM. Sensors 20(16):4636

[43] Xie et al., 2019. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. IEEE Communications Surveys and Tutorials, 21(3):2794– 2830.

[44] Falco et al., 2018. A master attack methodology for an AI-based automated attack planner for smart cities. IEEE Access, 6:48360-48373

[45] Hutchins et al. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. 6th International Conference on Information Warfare and Security, 2011.

[46] CAPEC. Common attack pattern enumeration and classification. Available on-line at: https://capec.mitre.org/ [Accessed: Nov. 05, 2020]

[47] MITRE ATT&CK. Common vulnerabilities and exposures. Available on-line at: https://attack.mitre.org/ [Accessed: Nov. 05, 2020]

[48] Garcia-Font et al., 2015. An architecture for the analysis and detection of anomalies in smart city WSNs. IEEE International Smart Cities Conference (ISC2).

[49] On evaluating stream learning algorithms, João Gama, Raquel Sebastião, Pedro Pereira Rodrigues

[50] "Web Services Architecture". World Wide Web Consortium. 11 February 2004. 3.1.3 Relationship to the World Wide Web and REST Architectures. Retrieved 29 September 2016.

10.2 Perception by stakeholders

[1] Anderson, J. E. (2003). Public policymaking: An introduction. Boston: Houghton Mifflin Company, pp. 1 – 34.

[2] Brown, J., & Doucet, M. (2020). “Chief, I think we can make this work.” Perceptions of successes and failures in technology implementation from Canadian police leaders. Journal of Community Safety and Well-Being, 5(4), 171-177

[3] Choong, Y, Dawkins, S., Furman, S., Greene, K.K., Spickard Prettyman, S., Theofanos, M.F. Voices of First Responders – Identifying Public Safety Communication Problems: Findings from User-Centered Interviews. Phase 1, Volume 1. NISTIR 8216 (2018). https://doi.org/10.6028/NIST.IR.8216

[4] Dawkins, S., Choong, Y., Theofanos, M., Greene, K., Furman, S., Steves, M., and Spickard- Prettyman, S. Voices of First Responders – Examining Public Safety Communication Problems and Requested Functionality, Findings from User-Centered Interviews. Phase 1, Volume 2.1. NISTIR 8245 (2019). http://doi.org/10.6028/NIST.IR.8245

[5] Greene, K. K., Dawkins, S., Spickard-Prettyman S., Konkol, P., Theofanos, M. F., Mangold, K., Furman, S., Choong, Y., Steves, M. P., Voices of First Responders—Nationwide Public Safety Communication Survey Methodology: Development, Dissemination, and Demographics. Phase 2, Volume 1. NISTIR 8288 (2020). http://doi.org/10.6028/NIST.IR.8288

[6] Greene, K. K., Dawkins, S., Theofanos, M., Steves, M., Furman, S., Choong, Y., and Spickard-Prettyman, S. Voices of First Responders—Examining Public Safety Communication from the Rural Perspective, Findings from User-Centered Interviews,Phase 1, Volume 3. NISTIR 8277 (2019). http://doi.org/10.6028/NIST.IR.8277

[7] Steves, M., Theofanos, M. F., Choong, Y., Dawkins, S, Furman, S., Greene, K. K., Spickard Prettyman, S. Voices of First Responders – Examining Public Safety Communication from the Perspective of 9-1-1 Call Takers and Dispatchers Findings from User-Centered Interviews, Phase 1, Volume 4. NISTIR 8295. (2020). https://doi.org/10.6028/NIST.IR.8295

[8] Dawkins, S., Greene, K.K., and S., Prettyman. (2020). Voices of First Responders – Nationwide Public Safety Communication Survey Findings: Mobile Devices, Applications, and Futuristic Technology, Phase 2, Volume 2. NISTIR 8314, August, 2020. https://doi.org/10.6028/NIST.IR.8314

[9] Chong, Y. and Salvedy G. Voices of First Responders – Applying Human Factors and Ergonomics Knowledge to Improve the Usability of Public Safety Communications Technology, Phase 1, Volume 5, NISTIR 8340, February, 2021. https://doi.org/10.6028/NIST.IR.8340

10.3 Technical issues

[1] Deloitte-NASCIO Cybersecurity Study, https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/DI_2018-Deloitte-NASCIO-Cybersecurity-Study.pdf

[2] Deloitte Insights, Making smart cities cybersecure Ways to address distinct risks in an increasingly connected urban future, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Report_making_smart_cities_cyber_secure.pdf

[3] The Biggest Smart City Security Challenges in 2019, https://blog.mobility.here.com/smart-city-challenges

[4] Smart Cities: Threat and Countermeasures, https://www.rambus.com/iot/smart-cities/

[5] S. Singh, P. K. Sharma, S. Y. Moon and J. H. Park, "Advanced lightweight encryption algo-rithms for IoT devices: Survey, challenges and solutions.," Journal of Ambient Intelligence and Humanized Computing, pp. 1-18, 2017.

[6] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier and R. Dahab, "NanoECC: Testing the limits of elliptic curve cryptography in sensor networks," European conference on Wireless Sensor Networks, pp. 305-320, 2008.

[7] A. Boyaci and A. M. Abed, "A Lightweight Cryptography Algorithm for Secure Smart Cities and IOT," 2020.

[8] S. S. Dhanda, B. Singh and P. Jindal, "Lightweight Cryptography: A Solution to Secure IoT," Wireless Personal Communications, pp. 1-34, 2020.

[9] A. Duru and I. Karas, "IOT Enabled Indoor Navigation System Design for Emergencies," International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, vol. 42, no. 4/W12, 2019.

[10] N. K. Singh, "Near-field Communication (NFC)", Information Technology and Libraries," Information Technology and Libraries, vol. 39, no. 2, 2020.

[11] D. Gravrel, "How to Develop Connected, Profitable, Smart Cities with WiFi", The Smart City Journal, https://www.thesmartcityjournal.com/en/technology/538-how-to-develop-connected-profitable-smart-cities-with-wifi, retrieved 2020.

[12] Z. Qadir, F. Al-Turjman, M. A. Khan and T. Nesimoglu, "ZIGBEE based time and energy efficient smart parking system using IOT," in 2018 18th mediterranean microwave symposium (MMS, IEEE, 2018, pp. 295-298.

[13] SEPURA industry report on TETRA communications for public safety: Past, present and future, 2018. (https://assets.markallengroup.com/article-images/192421/TETRA%20Communications%20For%20Public%20Safety.pdf)

[14] D. Jackson, "UK public safety's transition from TETRA to LTE-based ESN targeted for 2024 or 2025, Home Office officials say", UK Parliament News, September 15, 2020.

[15] Deloitte, "5G Smart Cities White Paper", June 2020. https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology-media-telecommunications/deloitte-cn-tmt-empowering-smart-cities-with-5g-white-paper-en-200702.pdf

[16] S. Ijaz, M. A. Shah, A. Khan and M. Ahmed, "Smart cities: A survey on security concerns", International Journal of Advanced Computer Science and Applications," International Journal of Advanced Computer Science and Applications, vol. 7, no. 2, pp. 612-625, 2016.

[17] European Air Quality Index. https://airindex.eea.europa.eu/Map/AQI/Viewer/#. Site visited december 2020

[18] Federation of American Scientists, 2013

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

[19] Eto A., Kanatami Y. 2018. Countering Bioterrorism: Current Status and Challenges - A Focus on Pharmaceutical Products and Vaccines. ADC Letter for Infectious Disease Control 5(2):50-52

[20] Moser, R., White G., Lewis-Younger C.R., Garrett L.C. 2001. Preparing for expected bioterrorism attack. Millitary medicine 166(5): 369-374

[21] New Security Guidance for Early Adopters of the IoT https://cloudsecurityalliance.org/download/new-security-guidance-for-early-adopters-of-the-iot/

[22] IoT Security Guidelines for Service Ecosystems http://www.gsma.com/connectedliving/wp-content/uploads/2016/11/CLP.12-v1.1.pdf

[23] Security Challenges for IoT and Smart City Systems and Applications, https://planejamento.rs.gov.br/upload/arquivos/201906/04154223-3-2-fabiano-smart-gov.pdf

[24] L. Cui, G. Xie, Y. Qu, L. Gao and Y. Yang, “Security and privacy in smart cities: Challenges and opportunities,” IEEE access, vol. 6, pp. 46134--46145, 2018.

[25] Future Directions in Human Machine Teaming https://basicresearch.defense.gov/Portals/61/Future%20Directions%20in%20Human%20Machine%20Teaming%20Workshop%20report%20%20%28for%20public%20release%29.pdf

[26] Y. Taigman, M. Yang, M. Ranzato and L. Wolf, “DeepFace: Closing the Gap to Human-Level Performance in Face Verification,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2014, pp. 1701-1708.

[27] J. Valentino-DeVries, “How the Police Use Facial Recognition, and Where it Falls Short,” The New York Times, 2020.

[28] A. Jarmanning, "Boston Bans Use of Facial Recognition Technology. It's the 2nd-Largest City to Do So", wbur.org, June 24, 202

[29] Interoperability of real-time public safety data: Challenges and possible future states https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8255.pdf

[30] FIWARE: The Open Source Platform for Our Smart Digital Future, https://www.fiware.org/

[31] Standards for M2M and the Internet of Things, https://www.onem2m.org/

[32] Blog: Future-proof smart cities: the case of Bordeaux, https://aioti.eu/blog-future-proof-smart-cities-the-case-of-bordeaux/

[33] Technical report: Adaptation of oneM2M for Smart City - http://www.onem2m.org/component/rsfiles/download-file/files?path=Draft_TR%255CTR-0036-Smart_City-V0_3_0.doc

[34] ETSI White Paper No. 31NGSI-LD API:for Context Information Management, https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp31_NGSI_API.pdf

[35] Clearview AI: Face-collecting company database hacked, https://www.bbc.com/news/technology-51658111

[36] Dutch Hackers Found a Simple Way to Mess With Traffic Lights, https://www.wired.com/story/hacking-traffic-lights-netherlands/

[37] Hack of D.C. police cameras was part of ransomware scheme, prosecutors say, https://www.washingtonpost.com/local/public-safety/attack-on-dc-police-security-cameras-had-broad-implications/2018/07/24/7ff01d78-8440-11e8-9e80-403a221946a7_story.html

[38] NESAS Security Assurance Specifications, https://www.gsma.com/security/nesas-security-assurance-specifications/

[39] NIST Special Publication 800-207 Zero Trust Architecture, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[40] Wilfred 1991 Physical Methods for Microorganisms Detection. Floride: CRC Press

[41] Pendlebury & Pickard. (1997). Examining ways to capture airborne microorganisms. Cleanrooms International, 1: 15-30

[42] Wang Z., Reponen T., Grinshpun S.A., Gorny R.L., Willeke K. (2001). Effect of sampling time and humidity on the bioefficiency of filter samplers for bioaerosol collection. Journal of Aerosol Science 32:661-674

[43] Durand K.T.H., Muilenberg M.L., Burge H.A., Seixas N.S. (2002) Effect on sampling time on the culturability of airborne fungi and bacteria sampled by filtration. Ann Occup Hyg 46: 113–118

[44] Verreault et al. (2008). Methods for Sampling of Airborne Viruses. Microbiol Mol Biol Rev., 72(3): 413–444

[45] Buttner, M.P. and al. 1997. Sampling and Analysis of Airborne Microorganisms. In Manual of Environmental Microbiology, edited by C. J. Hurst. ASM Press, Washington, DC, pp. 629-640

[46] Mathieu et al. (2009). Évaluation de biocollecteurs pour la détection de légionelles. Salles propres et maîtrise de la contamination, 35-40

[47] A Cyberattack Hobbles Atlanta, and Security Experts Shudder, https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

[48] Smart City Security: Atlanta Cyberattack Cripples City, https://www.iotworldtoday.com/2018/04/05/smart-city-security-atlanta-cyberattack-cripples-city/

[49] US charges Iranian 'SamSam' hackers, https://www.bbc.com/news/technology-46381033

[50] Johannesburg refuses to pay ransom after cyberattack, https://www.smartcitiesdive.com/news/johannesburg-refuses-to-pay-ransom-after-cyberattack/566120/

[51] https://www.usine-digitale.fr/article/la-cyberattaque-du-chu-de-rouen-serait-bien-d-origine-criminelle.N908519

[52] The Düsseldorf Cyber Incident, https://www.ifsh.de/en/news-detail/the-duesseldorf-cyber-incident

[53] Ten Ways to Protect Your City from Cyberattacks, https://www.nlc.org/article/2019/10/21/ten-ways-to-protect-your-city-from-cyberattacks/

[54] https://en.wikipedia.org/wiki/Pilot_error

[55] W. Choi, K. Moon and Y. Yoo, "Air traffic volume and air traffic control human errors," Journal of Transportation Technologies, vol. 1, pp. 47-53, 2011.

[56] McKinsey Report: Increasing FDNY's Preparedness, https://web.archive.org/web/20100603212555/http://home2.nyc.gov/html/fdny/html/mck_report/toc.shtml

[57] A Black man in Detroit was arrested and detained from 30 hours after being falsely identified by facial recognition, https://www.businessinsider.com/black-man-arrested-after-being-falsely-identified-by-facial-recognition-2020-6

[58] NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

[59] Boston just became the latest city to ban use of facial recognition technology, https://www.businessinsider.com/boston-bans-government-use-of-facial-recognition-technology-2020-6?r=US&IR=T

[60] Center for disease control and prevention. Emergency Preparedness and Response. Bioterrorism Agents/Diseases. https://emergency.cdc.gov/agent/agentlist-category.asp. Site visited december 2020

[61] Ludovici G.M., Gabbarini V., Cenciarelli O., Malizia A., Tamburrini A., Pietropaoli S., Carestia M., Gelfusa M., Sassolini A., Di Giovanni D., Palombi L., Bellecci C., Gaudio P. 2015. A review of techniques for the detection of biological warfare agents. Defence S&T technical bulletin, 8(1): 17-26

[62] Dunbar, J.; Pillai, S.; Wunschel, D.; Dickens, M.; Morse, S.A.; Franz, D.; Bartko, A.; Challacombe, J.; Persons, T.; Hughes, M.A.; et al. Perspective on Improving Environmental Monitoring of Biothreats. Front. Bioeng. Biotechnol. 2018, 6, doi:10.3389/fbioe.2018.00147.

[63] Brad Smith. A moment of reckoning: the need for a strong and global cybersecurity response, https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

[64] SolarWinds Report - https://sec.report/Document/0001628280-20-017451/

10.4 Operational issues

[1] Lowenthal, Mark. Intelligence: From Secrets to Policy (Los Angeles: Sage, 2017), 156.

[2] ERGO-CSEL 01-TR-01 2001. Aiding the Intelligence Analyst in Situations of Data Overload: From Problem Definition to Design Concept Exploration. Ohio: Institute for Ergonomics/Cognitive Systems Engineering Laboratory Report.19.

[3] Petersen, Karen Lund and Tjalve, Vibeke Schou. "Intelligence expertise in the age of information sharing: public-private ‘collection’ and its challenges to democratic control and accountability", Intelligence and National Security, 2018, 33:1, (24 April 2017): 21-35. DOI:10.1080/02684527.2017.1316956. 21-22.

[4] Dialogue meeting with local police intelligence officers in Trondheim, Norway (March 2021).

[5] Treverton, Gregory F. "The Intelligence Challenges of Hybrid Threats". Center for Asymmetric Threat Studies (CATS). 2018, 4. https://www.diva-portal.org/smash/get/diva2:1250560/FULLTEXT01.pdf

[6] Assemblée Nationale N° 3922, Rapport fait au nom de la commission d'enquête: relative aux moyens mis en oeuvre par l’État pour lutter contre le terrorisme depuis le 7 janvier 2015. 2016. https://www.assemblee-nationale.fr/14/rap-enq/r3922-t1.asp

[7] Hulnick, Arthur S. "What's wrong with the Intelligence Cycle." Intelligence and National Security, 2006, 21:6 (December 22, 2006): 959-979. DOI:10.1080/02684520601046291. 963

[8] NOU 2012: 14. Rapport fra 22.juli-kommisjonen. Oslo: Departementenes servicesenter Informasjonforvaltning.https://www.regjeringen.no/contentassets/bb3dc76229c64735b4f6eb4dbfcdbfe8/no/pdfs/nou201220120014000dddpdfs.pdf

[9] Intelligence collection should not be understood as a "neutral and value-blind practice" according to Petersen an Tjalve. Petersen and Tjalve, "Intelligence expertise in the age of information sharing", 27.

[10] Andreas Lutsch (2020) "Focusing on Practices of Intelligence Analysis within the EU", *International Journal of Intelligence and CounterIntelligence*, 33:3, 499-505, DOI:10.1080/08850607.2020.1754671. 503.

[11] Donald, F. "Information processing challenges and research directions in CCTV surveillance." *Cognition, Technology and Work*, (2019): 487-496. 492. DOI:10.1007/s10111-018-0535-6

[12] Homeland Security. "Planning Considerations: Complex Coordinated Terrorist Attacks". 2018.1-2. https://www.fema.gov/sites/default/files/2020-07/planning-considerations-complex-coordinated-terrorist-attacks.pdf

[13] Krasmann, Susanne, Hentschel, Christine "‘Situational awareness’: Rethinking security in times of urban terrorism." *Security Dialogue* 2019, 2 (January 31, 2019): 181-197,182. DOI:10.1177/0967010618819598

[14] The sapeurs-pompiers brigade of Paris (BSPP) translates as the Paris Fire Brigade and is a French Army unit which serves as the primary fire and rescue service for Paris, the city's inner suburbs and certain sites of national strategic importance. https://www.pompiersparis.fr/fr/

[15] This unit is a specialized unit part of the Police Nationale. http://le.raid.free.fr/medecin.htm

[16] The InterAgency Board. "Improving Active Shooter/Hostile Event Response. Best Practices and Recommendations for Integrating Law Enforcement, Fire, and EMS". 2015.

https://www.interagencyboard.org/sites/default/files/publications/External%20IAB%20Active%20Shooter%20Summit%20Report.pdf

[17] Kumbhar, A., Koohifar, F., Güvenç, I., Mueller, B. "A Survey on Legacy and Emerging Technologies for Public Safety Communications". IEEE Communications surveys & tutorials, 19(1), 2017.

[18] Hawkins, D. "Law Enforcement tech guide for Communications Interoperability. A Guide for Interagency Communications Projects". 2013, p. 15. https://www.cisa.gov/sites/default/files/publications/LawEnforcementTechGuide_CommunicationsInteroperability_2013_508C.pdf

[19] National Institute of Standards and Technology (NIST). "Interoperability of Real-Time Public Safety Data: Challenges and Possible Future States", 2019. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8255.pdf

[20] Human Factors in CCTV Control Rooms: a best practice guide. https://www.cpni.gov.uk/system/files/documents/aa/e6/human-factors-in-CCTV-control-rooms-a-best-practice-guide.pdf

[21] Milch, V. & Laumann, K. (2016) Interorganizational complexity and organizational accident risk: A literature review. Safety Science, 82, 9-17.

[22] Sætren GB, Laumann K (2014) Effects of trust in high-risk organizations during technological changes. Cognition, Technology & Work 17:131–144.

[23] Antonovsky, A., Pollock, C., & Straker, L. (2014). Identification of the human factors contributing to maintenance failures in a petroleum operation. Human factors, 56(2), 306-321.

[24] https://www.nrk.no/norge/pst-har-utviklet-terror-sokemotor-1.8392238 (accessed on 20.05.2021)

[25] https://www.adressa.no/nyheter/innenriks/article6646983.ece (accessed on 20.05.2021)

[26] Joh, E. (2019). Policing the smart city. *International Journal of Law in Context, 15*(2), 177-182. doi:10.1017/S1744552319000107

[27] Anderson, David, Independent assessment of MI5 and police internal reviews: Attacks in London and Manchester March-June 2017, Unclassified, December 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664682/Attacks_in_London_and_Manchester_Open_Report.pdf

[28] Myndighet för Samhällskyld og beredskap, Utvärdering av hanteringen av attentatet i Stockholm 7 april 2017 Redovisning av regeringsuppdrag Ju2017/05643/SSK. https://www.msb.se/RibData/Filer/pdf/28471.pdf

10.5 Ethical and legal issues

[1] AccessNow. One Year Under the EU GDPR, An Implementation Progress Report: State of play, analysis, and recommendations. AccessNow.org, 2019

[2] Article 29 Working Party, Opinion 4/2007 on the concept of personal data. 01248/07/EN WP 136.

[3] Artificial Intelligence Committee, AI in the UK: ready, willing and able? Report of Session 2017-19 - published 16 April 2017 - HL Paper 100

[4] Asilomar AI Principles (2017). Principles developed in conjunction with the 2017 Asilomar conference.

[5] Association for Computing Machinery (2018). ACM Code of Ethics and Professional Conduct: Affirming our obligation to use our skills to benefit society.

[6] Fjeld, J., Achten, N., Hilligoss, H., Nagy, A.C., Srikumar, M. (2020). Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI. Berkman Klein Center for Internet & Society at Harvard University. Research Publication No. 2020-1

[7] Boehm, F. (2012). Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level. Berlin: Springer-Verlag

[8] Brundage, M. and others (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation. Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, OpenAI.

[9] Bundesministerium des Innern, für Bau und Heimat, Bundesministerium der Justiz und für Verbraucherschutz (2018). The Federal Governments key questions to the Data Ethics Commission. 5 June 2018

[10] Cate, F.H., Dempsey, J.X. (eds.) (2017). Bulk Collection: Systematic Government Access to Private-Sector Data. Oxford: Oxford University Press

[11] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407.

[12] Clever, S., Crago, T., Polka, A., Al-Jaroodi, J., Mohamed, N. (2018). Ethical Analyses of Smart City Applications. *Urban Sci*. 2018, 2, 96

[13] Coastal Urban Development through the Lenses of Resiliency (CUTLER) (2018). This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 770469

[14] Coeckelbergh, M. (2020). AI Ethics. Cambridge: The MIT Press.

[15] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, OJ L 69, 13.3.2018, p. 23–43

[16] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

[17] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Protocol 2018 (CETS No. 223).

[18] Corea, F. (2019). An Introduction to Data: Everything You Need to Know about AI, Big Data and Data Sciences. Cham: Springer Nature.

[19] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p.37, amended by: Directive 2006/EC of the European Parliament and of the Council of 15 March 2006, OJ L 105, p. 54, and, Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ L 337, p. 337.

[20] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119 4.5.2016, p. 89

[21] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30

[22] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156, 19.6.2018, p. 43–7

[23] Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, OJ L 186, 11.7.2019, p. 122–137

[24] Van Eck, G.J.R. (2018). Emergency calls with a photo attached: The effects of urging citizens to use their smartphones for surveillance. In: Newell, B.C., Timan, T., Koops, B.-J. (eds) (2018) Surveillance, Privacy and Public Space. Routledge Publishing, 2018

[25] Empowering privacy and security in Non-Trusted Environments (WITDOM) (2017). This project has received funding from the European Union's Horizon 2020 research and innovation programme (H2020-ICT-2014-1) under grant agreement No. 64437.

[26] Ethics Advisory Group 2018 Report, Towards a digital ethics, available at: https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf (12th January 2021)

[27] European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The European Agenda on Security. COM(2015) 185 final

[28] European Commission. Communication for the Commission to the European Parliament, the European Council and the Council, Eleventh progress report towards an effective and genuine Security Union, COM/2017/0608 final

[29] European Commission. Communication from the Commission to the European Parliament, the European Council and the Council, the European Economic and Social Committee and the Committee of the Regions, Coordinated Plan on Artificial Intelligence, COM(2018) 795 final

[30] European Commission. Ethics and data protection. 14 November 2018.

[31] European Commission. European Group on Ethics in Science and New Technologies. Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems. Brussels, 2018

[32] European Commission. Independent High-Level Expert Group on Artificial Intelligence, European Commission. Ethics Guidelines for Trustworthy AI. Brussels, 2019

[33] European Commission. Report from the Expert Group on Liability and New Technologies – New Technologies Formation. Liability for Artificial Intelligence and other emerging digital technologies. European Union, 2019

[34] European Commission, 2020a. Report from the Commission to the European Parliament, the European Council and the Council, the European Economic and Social Committee, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final

[35] European Commission, 2020b. White Paper: On Artificial Intelligence – a European approach to excellence and trust, COM(2020) 65 final

[36] European Commission for the Efficiency of Justice, European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. 31st CEPEJ plenary meeting, Strasbourg, 2018.

[37] European Convention of Human Rights, Council of Europe, 1953

[38] European Data Protection Board (2020). Statement on restrictions on data subject rights in connection to the state of emergency in Member States. Adopted on 2 June 2002.

[39] European Data Protection Supervisor, Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 1.0. 15 November 2020

[40] European Data Protection Supervisor, Opinion 4/2015, Towards a new digital ethics Data, dignity and technology, 2015, available at: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf (12th January 2021)

[41] European Union Agency for Fundamental Rights, Council of Europe (2018). Handbook on European data protection law, 2018 edition. Luxembourg: Publications Office of the European Union.

[42] Evas, Tatjana. European framework on ethical aspects of artificial intelligence, robotics and related technologies: European added value assessment. European Parliament: European Parliamentary Research Service, PE 654.179, 2020

[43] Feldstein, S. (2019). The Global Expansion of AI Surveillance. Washington: Carnegie Endowment for International Peace

[44] Ferguson, A. G. (2017). The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. New York: New York University Press.

[45] Floridi, L. *et al.*, AI4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds and Machines (2018) 28:689–707.

[46] G20 (2019). Ministerial Statement on Trade and Digital Economy. G20 Osaka Summit, G20 Trade Meetings

[47] Harmonized Evaluation, Certification and Testing of Security products (HECTOS). Project funded by the European Community's Seventh Framework ProgrammeFP7/2007-2013 under Grant Agreement No 606861, 2015

[48] Institute of Electrical and Electronics Engineers (IEEE) (2019). Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. First Edition.

[49] Leslie, D. (2019). Understanding artificial intelligence ethics safety: A guide for the responsible design and implementation systems in the public sector. The Alan Turing Institute.

[50] Lorenz, P. (2020). AI Governance through Political Fora and Standards Developing Organizations: Mapping the actors relevant to AI governance. Berlin: Stiftung Neue Verantwortung

[51] Menzer, S., Rubba, C., Meißner, P., Nyhuis, D. (2015). Automated Data Collection with R: A Practical Guide to Web Scraping and Text Mining. West Sussex: John Wiley & Sons, Ltd

[52] Milaj, J., van Eck, G.J.R. (2019). Capturing license plates: police-citizen interaction apps from an EU data protection perspective. International Review of Law, Computers and Technology, 25 March 2019

[53] Montreal Declaration for a Responsible Development of Artificial Intelligence (2018). Announced at the conclusion of the Forum on the Socially Responsible Development of AI.

[54] OECD (2019). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449

[55] OECD (2020). The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector, available at: www.oecd.org/finance/Impact-Big-Data-AI-in-the-Insurance-Sector.htm

[56] Office of Homeland Security & Emergency Preparedness, City of New Orleans, available at: https://www.nola.gov/homeland-security/real-time-crime-center/ (12th January 2021)

[57] Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226 final - 2018/0107 (COD)

[58] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD)

[59] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final

[60] Purtova, N. (2018). Between GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public-Private Partnerships. International Data Privacy Law (2018)

[61] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final - 2018/0108 (COD)

[62] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, OJ L 141, 5.6.2015, p. 1–18

[63] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016

[64] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98

[65] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59–68

[66] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69

[67] Safe Data-Enabled Economic Development Horizon 2020 research and innovation programme (Safe-DEED), Grant Agreement No. 825225

[68] Shaping the ethical dimensions of smart information systems (SIS) – a European perspective (SHERPA) (2018). his project has received funding from the European Union's Horizon 2020 Research and Innovation Programme Under Grant Agreement no. 786641

[69] von Silva, B., Larsen, T. (2011). Setting the Watch: Privacy and the Ethics of CCTV Surveillance. Portland: Hart Publishing.

[70] Timmermans, H. (ed.) (2009). Pedestrian Behavior: Models, Data Collection and Applications. Bingley: Emerald Group Publishing Limited

[71] Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012

[72] United Nations Organization, Universal Declaration of Human Rights, General Assembly resolution 217 A

[73] United Nations Organization, High-Level Committee on Management. Personal Data Protection and Privacy Principles. 36th Meeting, October 2018

[74] Vogiatzaki, M., Zerefos, S., Tania, M.H. (2020). Enhancing City Sustainability through Smart Technologies: A Framework for Automatic Pre-Emptive Action to Promote Safety and Security Using Lighting and ICT-Based Surveillance. *Sustainability* 2020, 12, 6142.

[75] Voigt, Paul, von dem Bussche, Axel. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer. Cham: International Publishing, 2017

[76] Young, M., Katell, M., Krafft, P.M. (2019). Municipal surveillance regulation and algorithmic accountability. Big Data & Society, July-December 2019: 1-14.

[77] Zwitter, A. (2014). Big Data Ethics. Big Data & Society. July-December 2014; 1-6.

APPENDICES

A Detailed results from survey of public perception

A.1 Level of familiarity with the concept of Smart Cities

As can be noted from Figure 5, the largest share of the respondents (43.2%) have heard about the concept of Smart Cities, but they are not familiar with the details, followed by 36.3% of the respondents who are familiar with some Smart Cities technologies, and 20.5% who have never heard about it.

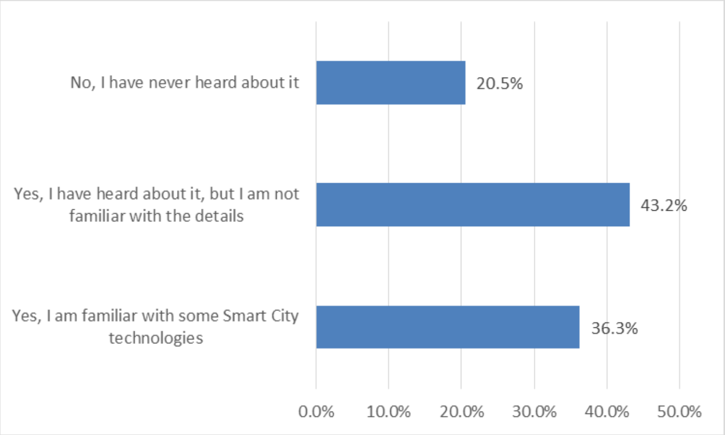

Figure 5. Familiarity with the concept of Smart Cities

There are statistically significant gender differences in this regard, since males are more likely to declare more knowledge about Smart Cities technologies (Table 9). For example, 43.1% of females have never heard about the concept, whereas among males this share amounts to 28.6%. As probably could have been expected, older respondents are less familiar with the concept. Namely, the average age of those who are not familiar with the concept is 54.7 yrs., while for those who are familiar with some of the technologies is about 41.6 yrs.

Table 9. Familiarity with the concept of Smart Cities – by gender

	No, I have never heard about it	Yes, I have heard about it, but I am not familiar with the details	Yes, and I am familiar with some Smart City technologies	Total
Male	335 (28.6%)	525 (44.8%)	311 (26.6%)	1171 (100.0%)
Female	580 (43.1%)	563 (41.8%)	204 (15.1%)	1347 (100.0%)
Total	915 (36.3%)	1088 (43.%)	515 (20.5%)	2518 (100.0%)

However, there are also statistically significant and substantial differences between the cities, as can be noted from Table 10. Namely, citizens of Padua expressed the highest, and citizens of Oslo and Zagreb the lowest level of familiarity. For instance, only 17.4% of Padua citizens declared no knowledge about the concept, while this number is 49.3% in Oslo and 47.1% in Zagreb. Citizens of Bucharest and Madrid positioned themselves somewhere in the middle.

Table 10. Familiarity with the concept of Smart Cities – by cities (%)

	Bucharest	Madrid	Oslo	Padua	Zagreb
Yes, I am familiar with some Smart City technologies	21.9	19.7	11.0	38.8	11.0
Yes, I have heard about it, but I am not familiar with the details	46.7	44.0	39.7	43.8	41.8
No, I have never heard about it	31.5	36.3	49.3	17.4	47.1

A.2 Perception of the necessity of using Smart Cities technology to improve urban services

The next question in the questionnaire was related to using technology to improve existing services provided by city institutions. For each of the areas listed below the participants expressed their opinion whether it is necessary to make use of digital Smart Cities technology to improve services in their cities. The first area that was offered was public transportation, and the data presented in Figure 6 reveal that 46.0% of citizens believe that it is highly necessary to use Smart Cities digital technologies in public transportation, while additional 30.7% think that it is necessary to do so.

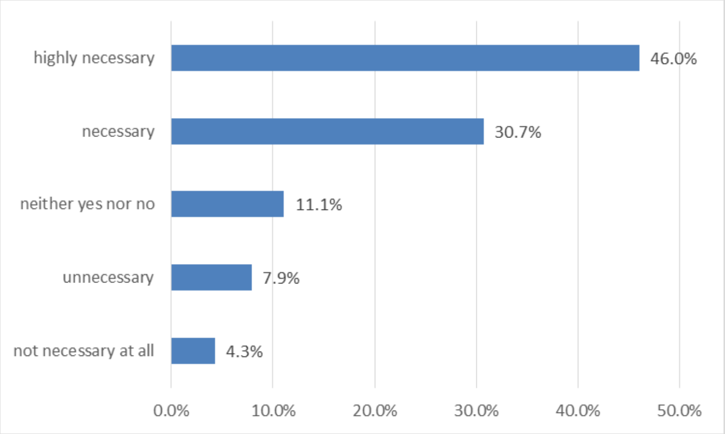

Figure 6. Necessity to use Smart Cities technology to improve public transportation

There is quite similar level of the necessity perception when it comes to the waste disposal, given that in this case as well about 75% of the citizens think that it is necessary or highly necessary to use Smart Cities technologies in this area.

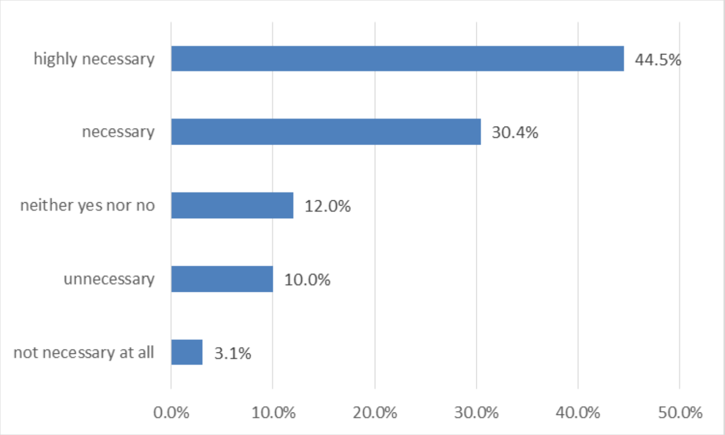

Figure 7. Necessity to use Smart Cities technology to improve waste disposal

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

About 68% of the respondents expressed their view that it is necessary or highly necessary to use Smart Cities technologies to improve energy efficiency and management (Figure 8).

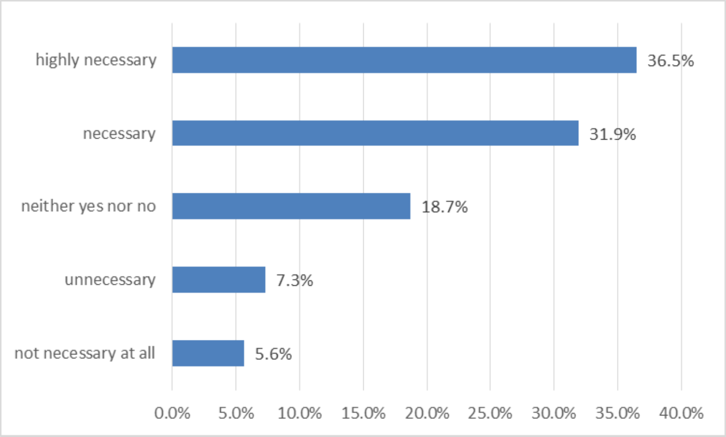

Figure 8. Necessity to use Smart Cities technology to improve energy efficiency and management

The perception of the necessity to use Smart Cities technology to improve management of healthcare is also very high – about 75% of the respondents think that this is necessary or highly necessary (Figure 9).

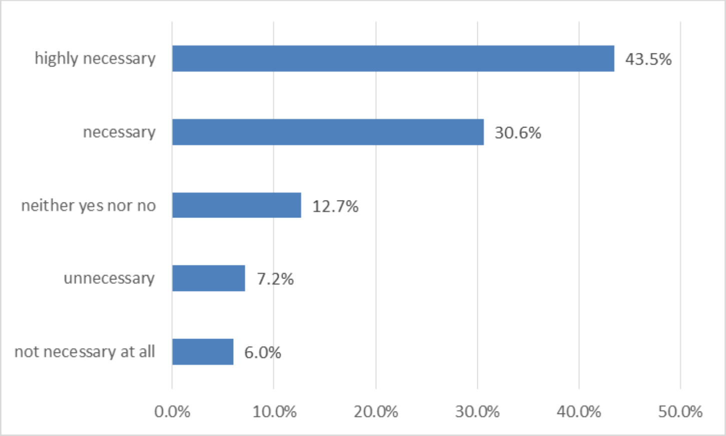

Figure 9. Necessity to use Smart Cities technology to improve smart management of healthcare

Interestingly, only about 58% of the citizens think that it is necessary or highly necessary to improve security through the use of digital Smart Cities technologies (Figure 10).

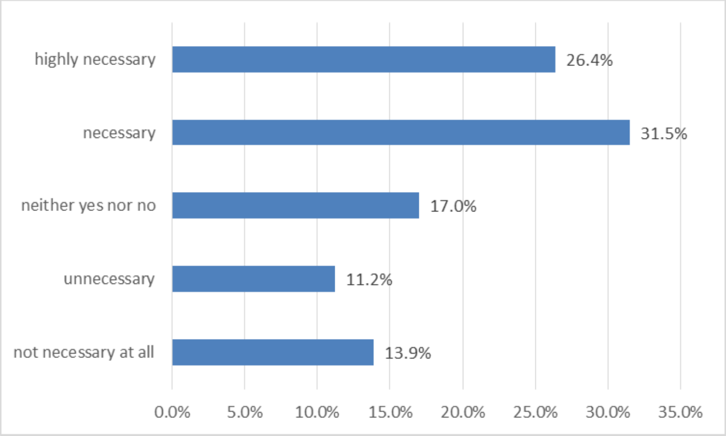

Figure 10. Necessity of using Smart Cities technology to improve security

And finally, there is also a high level of perception of necessity to use Smart Cities technology to improve warning system for high air pollution and other ecological services (Figure 11).

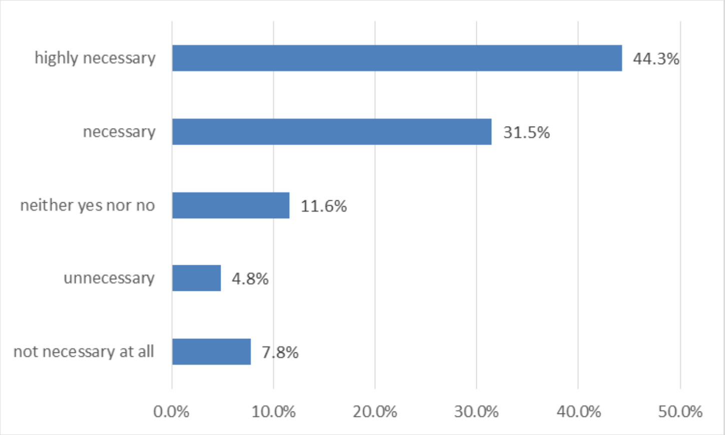

Figure 11. Necessity to use Smart Cities technology to improve warning systems for high air pollution and other ecological services

It is interesting to note that even though women expressed lower level of familiarity with the concept of Smart Cities technologies, they are more likely to think that some of the uses of Smart Cities technologies are important in comparison to men. For instance, energy efficiency and management (the average values are 3.91 vs 3.80, respectively), security (3.55 and 3.34, respectively) and warning systems for air pollution and other ecological purposes (4.08 vs. 3.90, respectively). There is only one significant correlation between respondent's ager and the necessity perception – older citizens think that the use of Smart Cities technology for better urban security is more important in comparison to younger citizens.

In the following table, the differences between the cities are shown. The analyses of variance showed that Padua citizens are the least likely to think that Smart Cities technology is needed in improving public transportation, waste disposal, energy efficiency and management, and warning systems for high air pollution and other ecological purposes. Citizens of Zagreb are least likely to express the need for Smart Cities technology in security and healthcare management. In all these cases citizens of Bucharest expressed the highest level of need for such technologies. Oslo and Madrid citizens expressed average level of need for such technologies.

Table 11. Perception of necessity of using Smart Cities technology to improve urban services – by cities (%)

	Not necessary at all	Unnecessary	Neither yes nor no	Necessary	Highly necessary	Mean
public transportation(for example, coordination of traffic lights)						
Bucharest	1.4	1.8	4.3	28.1	64.4	4.52
Madrid	2.6	3.8	5.4	32.7	55.6	4.35
Oslo	2.2	2.2	15.4	32.1	48.1	4.22
Padua	11.6	23.4	13.8	21.4	29.8	3.34
Zagreb	3.7	8.7	16.6	38.9	32.1	3.87
waste disposal (for example, information on the level of fullness of waste disposal containers)						
Bucharest	1.4	1.8	6.7	30.1	60.0	4.46
Madrid	3.0	4.0	7.8	28.3	57.0	4.32
Oslo	2.4	6.8	15.6	28.7	46.5	4.10

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

Padua	4.8	30.0	11.4	31.0	22.8	3.37
Zagreb	3.7	7.7	18.7	33.7	36.1	3.91
energy efficiency and management (for example, turning on the street lights during the night)						
Bucharest	3.7	4.5	6.7	31.1	53.9	4.27
Madrid	10.2	5.2	9.8	28.3	46.6	3.96
Oslo	9.6	9.0	19.6	23.6	38.3	3.72
Padua	0.8	8.4	43.6	39.0	8.2	3.45
Zagreb	4.2	9.5	14.0	37.4	35.0	3.90
smart management of healthcare (for example, using wearable devices to monitor your health at all times, online appointment making for the doctor's office, etc.)						
Bucharest	1.8	2.6	5.3	32.7	57.7	4.42
Madrid	5.2	5.2	5.6	25.1	59.0	4.27
Oslo	4.6	9.2	22.6	27.5	36.1	3.81
Padua	0.0	2.0	14.2	42.2	41.6	4.23
Zagreb	18.4	17.2	15.8	25.5	23.1	3.18
security (coverage of the entire city with surveillance cameras)						
Bucharest	2.0	3.0	6.3	31.3	57.5	4.39
Madrid	11.6	12.4	11.4	32.1	32.7	3.62
Oslo	18.6	14.6	23.4	20.6	23.0	3.15
Padua	0.4	3.4	29.0	59.8	7.4	3.70
Zagreb	36.9	22.7	15.2	14.2	11.0	2.40
warning systems for high air pollution, danger of floods, landslides, earthquakes etc.						
Bucharest	0.6	2.4	4.7	30.7	61.6	4.50
Madrid	2.4	4.0	8.6	22.9	62.2	4.38
Oslo	1.6	3.8	11.2	26.1	57.3	4.34
Padua	32.4	8.0	16.4	36.8	6.4	2.77
Zagreb	2.4	6.1	17.4	40.8	33.3	3.97

A.3 Trends in using Smart Cities technology and digital skills

The largest share of the participants – 49.4% of them – think that the use of Smart Cities technology in city management in the last five years has slightly improved. Further 11.7% think that such use has improved significantly.

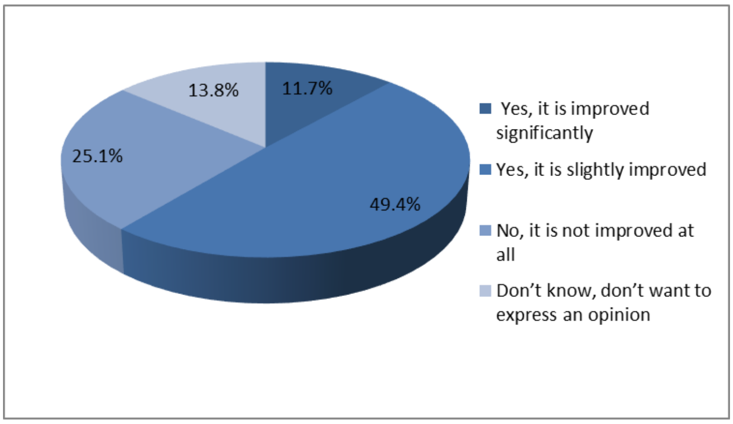

Figure 12. Trends in using Smart Cities technology

There are no gender differences in this regard, but older citizens are less likely to think that the application of Smart Cities technologies in their city has improved in the last five years. Namely, the average age of those who think that the situation has not improved is 52.2 yrs., while for the first two groups it amounts to about 47 yrs.

The survey participants from Bucharest and Zagreb are more often of an opinion that the situation in their city regarding the use of Smart Cities technologies has not improved. The participants from Padua largely think that the situation has been improving, but only slightly. The participants from Madrid, and especially Oslo, more often think that the situation has improved significantly, but in those two cities the share of the respondents who think that the situation has not improved at all is also substantial (19.3% and 17.8%, respectively).

Table 12. Trends in using Smart Cities technology – by cities (%)

	Bucharest	Madrid	Oslo	Padua	Zagreb
Yes, it is improved significantly	7.7	16.3	21.4	4.4	8.7
Yes, it is slightly improved	42.9	60.6	48.1	61.4	34.2
No, it is not improved at all	44.3	19.3	17.8	9.8	34.0
Don't know, don't want to express an opinion	5.1	3.8	12.8	24.4	23.1

The next question was related to the possible worries that the level of digital skills required for the use of urban services such as e-government, intelligent parking systems etc. will be too high and might prevent citizens from the possibility of using these urban services. From Figure 13 it can be concluded that such worries are not very substantial, given that almost 60% of the participants are not worried or not worried at all. However, 16.0% of the participants are worried and further 4.2% very worried in this regard.

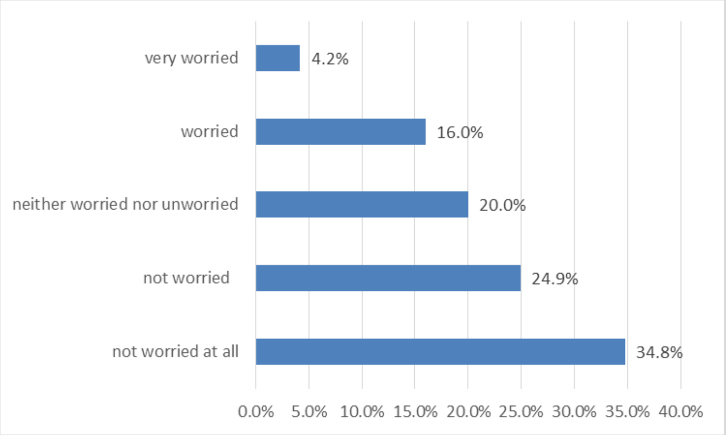

Figure 13. Worries about the increasing level of digital skills needed for Smart Cities services

Female respondents are more often worried about this issue than male – the averages are 2.39 and 2.20, respectively. As probably could have been expected, older citizens are more worried about their digital skills. As an illustration, the average age among those who are very worried is 56.2 yrs., and among those who are not worried at all 43.8 yrs.

As for the city differences, it is noticeable that citizens of Oslo, and especially Padua, are not worried because of the increasing level of needed digital skills, citizens of Madrid and Zagreb are the most likely to be worried, while Bucharest citizens are placed in the middle.

Table 13. Worries about the increasing level of digital skills needed for Smart Cities services – by cities (%)

	Bucharest	Madrid	Oslo	Padua	Zagreb
Not worried at all	28.0	17.7	48.3	68.0	12.6
Not worried	27.6	29.5	21.8	17.0	28.6
Neither worried nor unworried	24.4	17.7	16.2	7.2	34.3
Worried	16.1	28.7	9.2	5.0	20.9
Very worried	3.9	6.4	4.6	2.8	3.6

A.4 Sense of personal safety

In this part of the research the participants were first asked to estimate their general sense of safety taking into account all aspects of their daily life (traffic, crime, infrastructure, etc.). As shown inFigure 14, the citizens generally feel safe living in their city. Namely, only 11.0% of all participants declared that their city is unsafe or very unsafe.

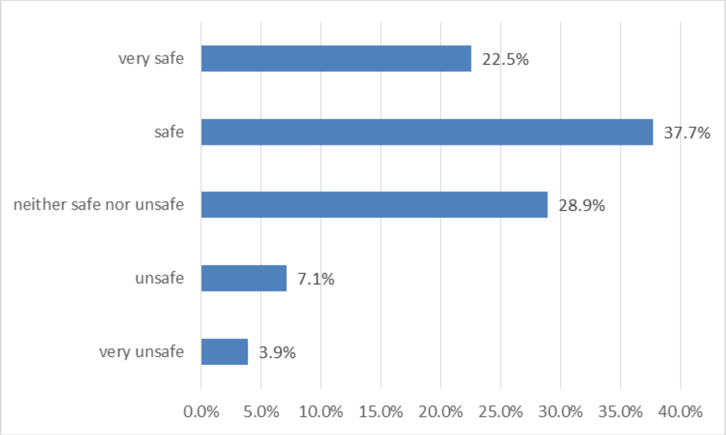

Figure 14. General perception of safety

Males feel statistically significantly more safe than females, but the differences are not very pronounced Even for females, the share of those who feel unsafe or very unsafe is not very large.

Table 14. General perception of safety – by gender

	Very unsafe	Unsafe	Neither safe or unsafe	Safe	Very safe	Total
Male	40 (3.4%)	73 (6.2%)	304 (26.0%)	460 (39.3%)	294 (25.1%)	1171 (100.0%)
Female	57 (4.2%)	106 (7.9%)	423 (31.4%)	489 (36.3%)	272 20.2%)	1347 (100.0%)
Total	97 (3.9%)	179 (7.1%)	727 (28.9%)	949 (37.7%)	566 (22.5%)	2518 (100.0%)

However, there are noticeable and substantial differences between the cities, with Bucharest citizens feeling the least secure on average. For instance, 30.7% of Bucharest citizens feel unsafe or very unsafe, while this goes only for 3.8% of Zagreb citizens, 3.8% of Padua citizens, 5.0% of Oslo citizens and 11.4% of Madrid citizens.

Table 15. General perception of safety – by cities (%)

	Bucharest	Madrid	Oslo	Padua	Zagreb
Very unsafe (1)	12.4	4.2	2.0	0.2	0.4
Unsafe (2)	18.3	7.2	3.0	3.6	3.4
Neither safe nor unsafe (3)	46.1	30.5	15.0	32.2	20.5
Safe (4)	18.5	39.4	38.1	51.0	41.6
Very safe (5)	4.7	18.7	41.9	13.0	34.1

The next question probed into the feeling of possible changes in the security level in the last couple of years. It can be noticed that about 60% of the participants estimate that the security level has not changed significantly, while the remaining participants are almost equally divided between those who think that the situation has improved and those who think that the situation has worsened.

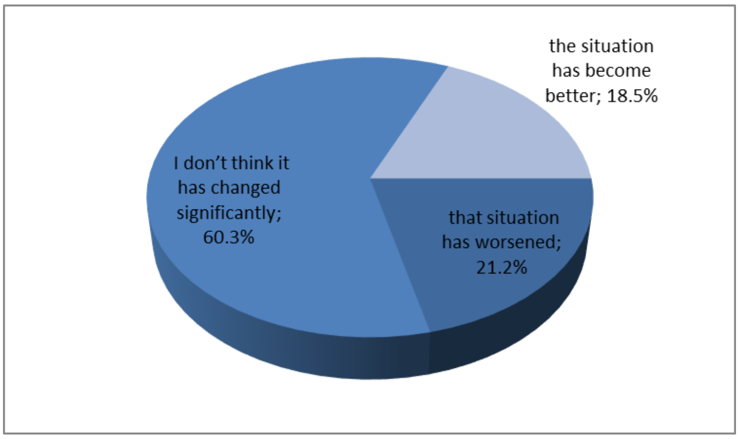

Figure 15. Recent change in the level of security

Gender differences in this regard are very similar as in the answers on the previous question. Namely, women are somewhat, even though not very substantially, more likely to believe that the safety situation has worsened.

Table 16. Recent change in the level of security – by gender

	The situation has worsened	I do not think it has changed significantly	The situation has become better	Total
Male	209 (17.8%)	707 60.4%)	255 (21.8%)	1171 (100.0%)
Female	324 (24.1%)	812 (60.3%)	210 (15.6%)	1346 (100.0%
Total	533 (21.2%)	1519 (60.3%)	465 (18.5%)	2517 (100.0%)

Compared to the general feeling of security, a similar pattern of the differences between the cities can be discerned from Table 17, even though it can be concluded that most citizens of Bucharest think that the (in)security level present in their city exists for some time. It is interesting to note that Padua citizens compare their current security situation much more favourably in comparison to the earlier situation. Precisely due to their answers the overall picture is not as bad as it could be, given that citizens of the other cities are more often inclined to think that the security situation in their city has worsened.

Table 17. Recent change in the level of security – by cities

	Bucharest	Madrid	Oslo	Padua	Zagreb
That situation has worsened	28.1	28.5	17.0	7.4	24.7
I don't think it has changed significantly	63.8	57.8	71.1	46.2	62.8
The situation has become better	8.1	13.7	12.0	46.4	12.5

A.5 Personal data misuse

In the next question, the participants were asked to indicate whether some of the digital privacy rights and identity thefts have happened to them personally. As can be seen fromFigure 16 the most often situation is use of data for unnecessary or unwanted purposes (49.5%), followed by violation of privacy rights (18.1%), identity theft or attempted identity theft (9.9%) and withdrawal of money from the account from an unknown source (9.8%).

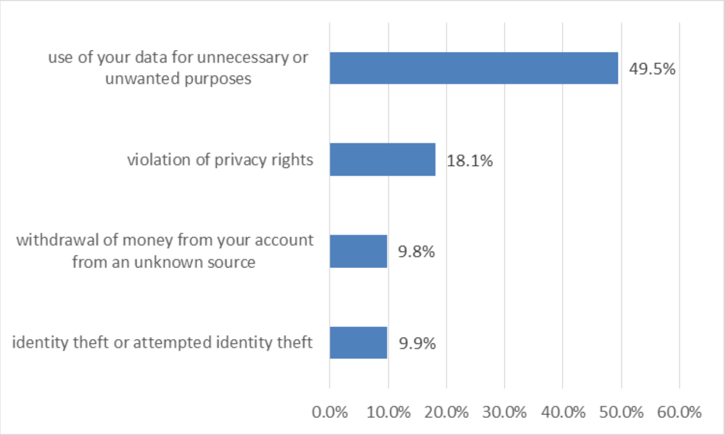

Figure 16. Violation of privacy rights and identity thefts („yes“ answers)

When it comes to gender differences, male more often reported the cases of violation of privacy rights and use of data for unnecessary or unwanted purposes. All cases of violations are more often reported by younger citizens, probably due to their more frequent use of various digital services.

Interestingly, there are substantial differences between the cities which participated in the survey. Zagreb citizens rarely reported such problems, especially when it comes to identity theft and withdrawal of money. The situation in Padua is similar, with the marked exemption of use of the personal data for unnecessary or unwanted purposes (marketing campaign, telephone directory, contact-lists of some companies, etc.). Namely, it seems that Padua citizens are very sensitive about such infringements of personal rights. The situations in Bucharest, Oslo and Madrid are very comparable, but the same exemption applies – Madrid citizens are also very sensitive about the above-mentioned use of personal data.

Table 18. Violation of privacy rights and identity thefts („yes“ answers) – by cities

	Bucharest	Madrid	Oslo	Padua	Zagreb
Identity theft or attempted identity theft	11.4	17.9	15.4	2.0	2.8
withdrawal of money from your account from an unknown source	9.6	16.9	16.8	2.2	3.6
violation of privacy rights	24.0	23.1	20.6	8.6	14.3
use of your personal data for unnecessary or unwanted purposes (marketing campaign, telephone directory, contact-lists of some companies, etc.)	42.3	70.7	44.1	72.8	18.2

Then the participants were asked whether they are worried that their personal information might be misused in the various situations. It is noticeable that the participants are most concerned for the security of their passwords on the internet – 15.7% of them are very worried about that. On the other hand, the least concern was expressed for surveillance camera footage – only 6.5% of the participants are very worried.

There are gender differences in only two situations – women are more concerned about purchases on the Internet (2.78 vs. 2.64) and putting personal data on Internet clouds (3.00 vs. 2.86). Younger citizens are

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

somewhat more concerned about the security of Internet passwords, Internet searches and surveillance camera footage.

Table 19. Concern about misuse of personal information (%)

	Not worried at all	Not worried	Neither worried nor unworried	Worried	Very worried	Do not know
payment with debit or credit cards in shops	31.0	23.6	18.9	19.3	7.2	1.2
use of information and comments from your social media accounts	23.2	21.9	21.2	22.5	11.2	7.1
data about my shopping activities collected by companies	16.0	28.5	22.3	23.1	10.1	0.9
security of your passwords on the internet	13.2	16.3	25.5	29.3	15.7	4.1.
your Internet searches	27.2	20.1	23.5	19.8	9.4	2.5
purchases on internet	25.7	18.1	24.0	23.4	8.7	4.2
surveillance camera footage	31.4	24.9	22.1	15.1	6.5	1.0
sharing your financial information between banks and insurance companies	15.1	26.4	23.0	24.6	10.8	0.8
putting your data on internet „clouds“	16.8	22.7	22.4	26.8	11.4	1.0

When it comes to the differences between the cities, it is conspicuous that Padua citizens are least concerned about any misuses of their personal information. On the other hand, Madrid citizens are the ones who are most often concerned, except in case of surveillance camera footage, where Bucharest citizens are more concerned. Zagreb citizens are also generally not very worried about the listed misuses, while Oslo and Bucharest are somewhat worried.

Table 20. Concern about misuse of personal information (the averages - ("1" is "Not worried at all", "5" is "Very worried") – by cities

	Bucharest	Madrid	Oslo	Padua	Zagreb
payment with debit or credit cards in shops	2.95	3.41	2.24	1.32	2.47
use of information and comments from your social media accounts	3.15	3.28	2.73	1.73	3.02
data about my shopping activities collected by companies	3.14	3.43	3.10	2.13	2.31
security of your passwords on the internet	3.40	3.77	3.23	2.32	3.15
your internet searches	3.10	3.16	2.94	1.31	2.70
purchases on internet	3.04	3.22	2.84	1.56	2.95
surveillance camera footage	2.87	2.68	2.29	1.52	2.66
sharing your financial information between banks and insurance companies	3.21	3.68	2.50	2.23	2.85
putting your data on internet „clouds“	3.26	3.55	2.79	2.01	3.07

And in the end, the survey participants were asked whether they are worried that some data about citizens collected by the Smart City services can be misused. Generally, more than 43% of all citizens worry or worry very much. Conversely, about 36% of citizens are not worried or not worried at all.

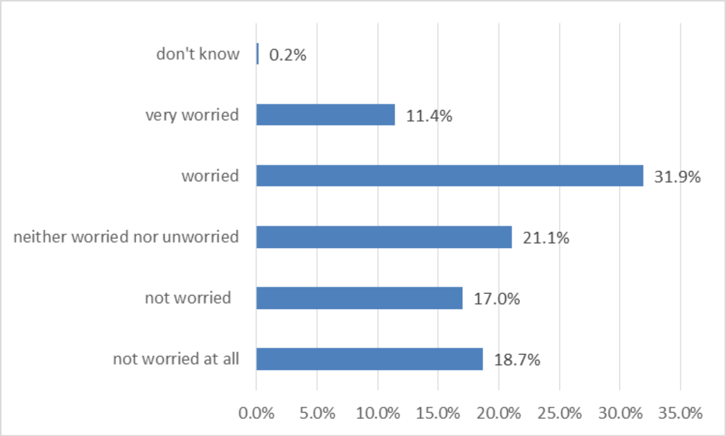

Figure 17. Concern over the misuse of the data collected by the Smart Cities services

Women are more worried about the possible misuses than men, but not very substantially – the averages are 3.02 and 2.98, respectively. Older citizens are more concerned about general possibility of misusing such data. For instance, the average age of those who are very worried is 51.3 yrs., while the average age of those who are not worried at all is 44.7 yrs.

The differences between the cities are patterned in a similar way as in the case of the concerns over misuses of one's own personal data, with some marked differences. In other words, Padua citizens are the ones who are the least concerned, while Madrid citizens are the most concerned. However, Zagreb citizens, largely unconcerned about the misuses of one's own data, are very concerned about possible misuses of the data collected by the Smart Cities services.

Table 21 .Concern over the misuse of the data collected by the Smart Cities services – by cities (%)

	Bucharest	Madrid	Oslo	Padua	Zagreb
Not worried at all	6.5	4.4	14.3	61.9	6.9
Not worried	20.3	6.2	25.2	22.2	11.0
Neither worried nor unworried	29.9	12.2	28.8	8.8	25.6
Worried	33.9	50.0	24.7	4.2	46.2
Very worried	9.4	27.3	7.0	2.8	10.3

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

B Detailed list of requirements for public safety solutions

The project uses an online tool (a customised SharePoint list) to register full details of all requirements.

The list of requirements presented in section 8 was generated from that list and showed a small subset of key fields for each of the requirements, including a reference to the integer "ID" of each requirement.

This appendix is provided for readers who may have a special interest in learning more about other detailed information related to each requirement. It is generated from the same online list but also shows other detailed fields. It is presented in order of "ID" number (#1, #2 etc), providing the link to the list in section 8.

<table>
<tr><td colspan="2"><b># 1 (<i>Category:</i></b> <i>Smart City Data;</i> <b><i>Type:</i></b> <i>10 Functional;</i> <b><i>Status</i></b><i>: 25 Under revision</i><b>)</b>
An Access Control methodology should handle access rights and data control.</td></tr>
<tr><td colspan="2">Different access privileges must be granted to data. Access control can be enforced at different points including the overall platform and tools. Each specific tool could have its own access control requirements.

Simplified Description: Traditional Access Control requirements. In IMPETUS we also have tools as entities that access to data in addition to users (city users, tool users etc.).</td></tr>
<tr><td><b>Source</b>: DoA (Section 1)</td><td><b>Dependencies</b>:</td></tr>
<tr><td><b>Importance</b>: 02 Required
03.05.2021 CPAD

important to guarantee that only the authorized people / systems could access to all the available data/ information. A limited authorized group of people could be able to modify data</td><td><b>Feasibility</b>:</td></tr>
</table>

<table>
<tr><td colspan="2"><b># 2 (<i>Category:</i></b> <i>Cyber;</i> <b><i>Type:</i></b> <i>10 Functional;</i> <b><i>Status</i></b><i>: 25 Under revision</i><b>)</b>
The data collection system should provide a standard based interface for data collection from data sources forming part of the monitored system</td></tr>
<tr><td colspan="2">Monitoring and audit of data forms the underlying system to conduct cybersecurity analysis of events and data exchanges between cybersecurity tools</td></tr>
<tr><td><b>Source</b>: WP3, T3.3</td><td><b>Dependencies</b>:</td></tr>
<tr><td><b>Importance</b>: 02 Required
03.05.2021 - CPAD

a standard based interface to collect data is important not only for cybersec but also for the adoption of the IMPETUS platform by other cities. --> CPAD would move this req to Deal breaker level</td><td><b>Feasibility</b>:</td></tr>
</table>

<table>
<tr><td><b># 3 (<i>Category:</i></b> <i>Smart City Data;</i> <b><i>Type:</i></b> <i>10 Functional;</i> <b><i>Status</i></b><i>: 25 Under revision</i><b>)</b>
The Access Control methodology should support sanitization policies that are enforced at ingestion</td></tr>
</table>

time before an access to data is granted.	
Sanitization policies that apply filtering (not including cryptographic) operations and data transformation to limit disclosure of personal data. They include operations like generalization, obfuscation, pruning. Simplified Description: In order to prevent privacy infringements, the data collected are subject to filtering while they are collected and before they are stored (ingestion) so that, where applicable, tools will have to deal (process and store) with privacy preserving data only	
Source: DoA	**Dependencies**:
Importance: 02 Required CPAD important	**Feasibility**:

# 4 (*Category:* *Cyber;* *Type:* *10 Functional;* *Status*: *25 Under revision*) The data collection system should collect system configuration information	
Configurability and parametrization of the monitoring and audit of cybersecurity framework	
Source: WP3, T3.3	**Dependencies**:
Importance: 02 Required CPAD impotant	**Feasibility**:

# 5 (*Category:* *Cyber;* *Type:* *10 Functional;* *Status*: *25 Under revision*) The IMPETUS Cybersecurity framework should provide a data collection system	
Analysis and prevention based on data analysis	
Source: WP3, T3.3	**Dependencies**:
Importance: 02 Required CPAD important	**Feasibility**:

# 6 (*Category:* *Cyber;* *Type:* *10 Functional;* *Status*: *25 Under revision*) The IMPETUS Cybersecurity framework must contain an information correlation engine	
Management of meta-alerts to merge and fuse cyber-security events	
Source: WP3, T3.3	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - it's critical that the platform could have an information correlation engine	**Feasibility**:

# 7 (*Category:* *Cyber;* *Type:* *10 Functional;* *Status*: *25 Under revision*)	

The information correlation engine must identify common information elements across the multi-source information received by the data collection system	
Fusion and merge of cybersecurity events reqiures from normalization and adaptation of multi-source data (e.g., from different cybersecurity tools)	
Source: WP3, T3.3	**Dependencies**:
Importance: 02 Required CPAD important	**Feasibility**:

# 8 (*Category:* *Cyber;* *Type:* *10 Functional;* *Status*: *25 Under revision*) The correlation results should be stored securely in an encrypted form	
Protection of the correlation process in terms of, e.g., integrity and disclosure attacks	
Source: WP3, T3.3	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - to be paid attention to the correlation process and results	**Feasibility**:

# 9 (*Category:* *Cyber;* *Type:* *10 Functional;* *Status*: *25 Under revision*) The IMPETUS Cybersecurity framework should provide a response system, to handle both proactive and reactive mitigation of threats and attacks	
Reaction-after-detection paradigm	
Source: WP3, T3.3	**Dependencies**:
Importance: 02 Required CPAD important - to provide a response system will make the cybersecurity tools more complete	**Feasibility**:

# 10 (*Category:* *Cyber;* *Type:* *10 Functional;* *Status*: *25 Under revision*) Mitigation actions proposed by the response system to handle threats and attacks should minimize the impact of such threats and attacks against the system	
Preempt attacks prior exploitation of vulnerabilities, and react when attacks are confirmed, while computing the performance of the response	
Source: WP3, T3.3	**Dependencies**:
Importance: 02 Required CPAD important - It's critical to minimize the impact of such threats and attacks against the system asap	**Feasibility**:

11 (*Category:* *Cyber;* *Type:* *10 Functional;* *Status*: *25 Under revision*)

Mitigation actions proposed by the response system to handle threats and attacks should minimize collateral damages of actions themselves	
Preempt attacks prior exploitation of vulnerabilities, and react when attacks are confirmed, while reducing the impact of such response in the system	
Source: WP3, T3.3	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - minimization of collateral damages is definitely critical	**Feasibility**:

# **12 (*Category:*** *Cyber;* ***Type:*** *10 Functional;* ***Status****: 25 Under revision*) The response system should benefit from the use of anomaly detection, in order to derive new attack patterns	
Responses can include, in addition to mitigation, derivation of new detection and response patterns	
Source: WP3, T3.3	**Dependencies**:
Importance: 03 Nice-to-have CPAD interesting - if itsn't too complcate it could provide added value	**Feasibility**:

# **13 (*Category:*** *Ethics;* ***Type:*** *40 Development;* ***Status****: 25 Under revision*) The development of an ethical guidelines must follow the Ethics Guidelines for Trustworthy AI	
The EU promulgates the EGTAI principles as the center-piece of its AI Ethics strategy. This relates to data collection and manipulation in security operations only.	
Source: DoA; D1.2, section 6; Ethics Guidelines for Trustworthy AI https://ec.europa.eu/futurium/en/ai-alliance-consultation	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - I think it's more or less mandatory	**Feasibility**:

# **14 (*Category:*** *Ethics;* ***Type:*** *40 Development;* ***Status****: 25 Under revision*) The ethical guidelines should thoroughly examine the ethical issues connected to the deployers category.	
This relates to data collection and manipulation in security operations only. This requirement is exclusively focused on tools that are closely examined within D5.1.	
Source: D5.1	**Dependencies**:
Importance: 01 Deal breaker CPAD very important	**Feasibility**:

<table>
<tr><td colspan="2"><b># 15 (<i>Category:</i></b> <i>Ethics;</i> <b><i>Type:</i></b> <i>40 Development;</i> <b><i>Status</i></b><i>: 25 Under revision</i><b>)</b>
The ethical guidelines should consider certain relevant aspects concerning the collection of data on one side, and privacy and personal data protection on the other</td></tr>
<tr><td colspan="2">This, depending on the partners' contributions in D5.1, may include considerations regarding: socio-technical environment, involuntary data collection and manipulation, mass surveillance, public safety and security, data as common good, legal aspects of personal data and privacy protection, ethical considerations with regard AI decision-making, ethical consideration regarding human operators and their interaction with AI, supervision and oversight.
This relates to data collection and manipulation in security operations only.</td></tr>
<tr><td><b>Source</b>: D5.1</td><td><b>Dependencies</b>:</td></tr>
<tr><td><b>Importance</b>: 01 Deal breaker
CPAD
very important</td><td><b>Feasibility</b>:</td></tr>
</table>

<table>
<tr><td colspan="2"><b># 16 (<i>Category:</i></b> <i>Ethics;</i> <b><i>Type:</i></b> <i>40 Development;</i> <b><i>Status</i></b><i>: 25 Under revision</i><b>)</b>
The ethical guidelines should consider the role of State, its obligation toward use of all available means (including technology) to protect its citizens, and its obligation to protect citizens personal data and privacy.</td></tr>
<tr><td colspan="2">This relates to data collection and manipulation in security operations only.
This requirement heavily depends on actual partners' contribution in D5.1.</td></tr>
<tr><td><b>Source</b>: D5.1</td><td><b>Dependencies</b>:</td></tr>
<tr><td><b>Importance</b>: 01 Deal breaker
CPAD
very important</td><td><b>Feasibility</b>:</td></tr>
</table>

<table>
<tr><td colspan="2"><b># 17 (<i>Category:</i></b> <i>Ethics;</i> <b><i>Type:</i></b> <i>40 Development;</i> <b><i>Status</i></b><i>: 25 Under revision</i><b>)</b>
Smart cites must develop a legal taxonomy for relevant data sets and flow down the requirements to all partners</td></tr>
<tr><td colspan="2">Impossible for all partners to know the source and requirments for each element of data and thus the proper way to handle them. Without this then the data will be unknowingly misused and violation of the GDPR will occur</td></tr>
<tr><td><b>Source</b>: D1.2, section 6; EU CUTLER project lesson learned</td><td><b>Dependencies</b>:</td></tr>
<tr><td><b>Importance</b>: 02 Required
CPAD
important - to pay attention to</td><td><b>Feasibility</b>:</td></tr>
</table>

<table>
<tr><td colspan="2"><b># 18 (<i>Category:</i></b> <i>Ethics;</i> <b><i>Type:</i></b> <i>10 Functional;</i> <b><i>Status</i></b><i>: 25 Under revision</i><b>)</b>
The ethical guidelines should assess the risks to fundamental data rights and data privacy.</td></tr>
<tr><td colspan="2">This relates to data collection and manipulation in security operations only.
This primarily relates to the tools utilized on IMPETUS Platform.</td></tr>
<tr><td><b>Source</b>: D5.1</td><td><b>Dependencies</b>:</td></tr>
<tr><td><b>Importance</b>: 01 Deal breaker</td><td><b>Feasibility</b>:</td></tr>
</table>

CPAD very important	

# 19 (*Category:* *Ethics; Type:* *30 Targeted use; Status: 25 Under revision*) Smart cities should inform citizens on risks of adopting integrated platforms and technologies	
Citizens surely benefit from a smart city in which an integrated platform for public safety and security operates. However, in light of acceptability, citizens must be informed about risks related to integrated platforms and technologies.	
Source: End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - this has to be considered in the project's scope (more than in the platform development), within the Ethical framework.	**Feasibility**:

# 20 (*Category:* *Operations; Type:* *40 Development; Status: 25 Under revision*) The security actors should lead the definition of new concepts of operation taking advantage of new technological capabilities.	
Source: 25/02 SINTEF find relevant reference	**Dependencies**: Related to #21
Importance: 02 Required CPAD important - new operations means new processes. This topic has to be considered both from Consortium people and from Cities end-users	**Feasibility**:

# 21 (*Category:* *Operations; Type:* *40 Development; Status: 25 Under revision*) The definition of new concepts of operation should identify and involve all relevant actors of security, covering daily activities as well as rare events.	
Source: 25/02 SINTEF find relevant reference	**Dependencies**:
Importance: 02 Required CPAD important - new operations means new processes. This topic has to be considered both from Consortium people and from Cities end-users	**Feasibility**:

22 (*Category:* *Technology integration; Type:* *20 Form; Status: 25 Under revision*) The platform interface should support different forms of interaction depending on situation and user

profile.	
When an event occurs, several people will receive the same alert information. Only some of them will be called to action. The visualization/interface MUST be profiled: e.g. if a earthquake occurs, only one SOC operator should be able to push a button and send a broadcast sms to all the citizens	
Source: End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD important that different people interacting with the platform have different views. We can currently think about at least 2 "horizontal" profiles (for physical SOC operators and IT analysts for Cyber sec) and 3 "vertical" profiles (end user, supervisor, admin)	**Feasibility**:

# 23 (*Category:* *Operations; Type:* *10 Functional; Status*: *25 Under revision*) Training plans for all relevant security actors should be created to address the concepts of operation with the public safety platform	
Actors should be made familiar with all major features and exposed to how they may deteriorate under exeptional strain	
Source: DoA; D1.2 section 5	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - nothing to add	**Feasibility**:

# 24 (*Category:* *Technology integration; Type:* *40 Development; Status*: *25 Under revision*) The IMPETUS platform should adapt a common terminology and symbology	
This to enable, as far as possible, standardized and unambiguous sharing and interpretation of data and information. Symbology here refers to the "representation or expression by means of symbols". Both user and solution provider need to agree on this common terminology and symbology. This requirement directly affects the platform development process and the resulting product.	
Source: D1.2, section 2	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - high risk to create confusion if the terminolgy and symbology are not shared and fully understood	**Feasibility**:

# 25 (*Category:* *Operations; Type:* *10 Functional; Status*: *25 Under revision*) Operations supported by the platform should comply with the national/international (if applicable) security frameworks, including legal and cyber related frameworks.	
Examples of legal and cyber related frameworks include GDPR and the EU cybersecurity certification framework.	
Source: D1.2, sections 4, 6	**Dependencies**:

Importance: 01 Deal breaker CPAD very important - the platform has to be fully compliant with GDPR or a stricter set of rules - likely, similar to other ones	**Feasibility**:

# 26 (*Category:* *Operations; Type:* *10 Functional; Status: 25 Under revision*) Smart cities should develop a methodology and process to monitor social media and open news sources.	
These sources of information will provide: 1. a large number of unfiltered leads and 2. a key to misinformation that the public is consuming and that needs to be dealt with at the earliest possible time,	
Source: Open source Multiple instances in D1.2, section 3	**Dependencies**:
Importance: 03 Nice-to-have interesting - it depends on which social media the platform will be able to monitor and how	**Feasibility**:

# 27 (*Category:* *Technology integration; Type:* *20 Form; Status: 25 Under revision*) To ensure synchronisation between security actors, the same interface visualizations and alerts should be provided to different SOCs.	
Several people MUST receive the same alert information at the same time. Ideally, the dashboard could be a kind of webpage, customizable with widgets, available for all the authorized people (e.g. home-banking dashboard). When some relevant event occurs, all the involved people receive the alert, so all of them are aligned. Then, only the right people take actions, according to the event management processes	
Source: End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - likely, similar to other ones	**Feasibility**:

# 28 (*Category:* *Technology integration; Type:* *10 Functional; Status: 25 Under revision*) The IMPETUS platform should allow for sharing of information to users from organisations which are not part of the IMPETUS operating environment through data exports, embedded views or guest access according to operational needs.	
Operational circumstances may necessitate the sharing of information from IMPETUS to external organisations during operation. To accomodate for this, the platform should have functionality which allows for sharing of information/embedding views to external organisations.	
Source: End-user perspective	**Dependencies**:
Importance: 02 Required CPAD important - likely, not easy	**Feasibility**:

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

# 29 (*Category:* *Smart City Data; Type: 40 Development; Status: 25 Under revision*) The change detector and event classifier stages (training/working) should be controlled remotely	
IMPETUS should provide a simple way to communicate also remotely with the change detector and event classifier in order to abilitate to explicitly switch from one state to another depending on the specific needs. Change detection and classification activate automatically while the corresponding training steps could be activated both manually and automatically. Simplified Description: Very technical requirements saying that we need to have access to the change detector backend to alter controlling parameters for training mainly	
Source: WP4, T4.1, D1.2 section 2 (intelligent layer)	**Dependencies**:
Importance: 02 Required CPAD important	**Feasibility**:

# 30 (*Category:* *Technology integration; Type: 30 Targeted use; Status: 25 Under revision*) The development of the platform and the specific tools should consider the connection of simultaneous users	
Cities have expressed the necesity of having access to the platform from different institutions and users.	
Source: End-user perspective	**Dependencies**:
Importance: 01 Deal breaker 23/03 CPAD very important - likely, similar to other ones	**Feasibility**:

# 31 (*Category:* *Technology integration; Type: 30 Targeted use; Status: 25 Under revision*) The public safety platform should be easily maintained by the technical staff of the city	
In case of "mild" failure, the platform capability should be easily restored firstly by internal technical personnel of the city	
Source: End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - we have to make our best effort to let the cities personnel to make adequate meinteinence to the platform: the risk is that after a short period, the cities quit and stop use the platform (or trash it)	**Feasibility**:

# 32 (*Category:* *Technology integration; Type: 30 Targeted use; Status: 25 Under revision*) The platform must be compatible with existing infrastructures for data collection adopted by the city	
Cities employs CCTVs networks, distributed sensors, ... and the platform must be able to accommodate all sources of data streams that can be available	
Source: DoA; D1.2 section 3	**Dependencies**:
Importance: 01 Deal breaker	**Feasibility**:

CPAD very important - inteconnection with Cities' equipment have to be undertaken via standard procedures/tools	

# 33 (***Category:*** *Technology integration;* ***Type:*** *20 Form;* ***Status****: 25 Under revision*) The IMPETUS platform/tools should provide appropriate transparency when it provides insight into the information sources and the calculations that contribute to the recommendations and predictions provided to a user.	
Observability provides transparency into what the IMPETUS platform/tools is doing relative to users' task progress within the City Command & Control context. Observability supports shared understanding of the problem to be solved and progress toward goals. The IMPETUS platform/tools are considered observable when it provides the right level of information, so the user understands its recommendations and predictions.	
Source: WP1 (human machine teaming), WP7 (user validation)	**Dependencies**:
Importance: 02 Required CPAD important	**Feasibility**:

# 34 (***Category:*** *Technology integration;* ***Type:*** *20 Form;* ***Status****: 25 Under revision*) The IMPETUS platform/tools should provide transparency of future intentions, states, and activities, as well as a projection of what the future situation will be if current trajectories are continued.	
The IMPETUS platform/tools must be able to direct the attention of the user to critical problem features, cues, indications, and warnings. The IMPETUS platform should communicate proactively when information becomes relevant.	
Source: WP1 (human machine teaming), WP7 (user validation)	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - likely, similar to other ones	**Feasibility**:

# 35 (***Category:*** *Technology integration;* ***Type:*** *20 Form;* ***Status****: 25 Under revision*) The IMPETUS platform should be able to provide different views from the available data according to the users' needs	
The information (provided and presented by/in the platform, using some kind of UI) should be presented to the user in a way that is best suited to that user. It should also be possible to view the information in different ways, assuming there will be different users of the platform, each with their own (different) needs.	
Source: End-user perspective	**Dependencies**: Related to #22
Importance: 02 Required CPAD important - likely, similar to other ones	**Feasibility**:

36 (***Category:*** *Technology integration;* ***Type:*** *20 Form;* ***Status****: 25 Under revision*)

The IMPETUS platform/tools should (proactively) direct the attention of users to critical problem features, cues, indications, and warnings when information become relevant.	
Exploring the Solution Space helps the user to leverage multiple views, knowledge, and solutions to jointly understand the problem space. The IMPETUS platform should be able to rapidly generate multiple distinct courses of action and give the user ways to rapidly compare those solutions. Both the user and the IMPETUS platform should be able to broaden or constrict the solution considerations to shift perspectives.	
Source: WP1 (human machine teaming), WP7 (user validation)	**Dependencies**:
Importance: 02 Required 08/04 THA (after review): Re: distinction between req 36 and 34: Req 36 is about the system adding emphasis in the interface towards the user (like alerts) which warrant additinal attention from the user. Req 34 is about showing future predictions. CPAD important	**Feasibility**:

# 37 (*Category:* *Technology integration; Type: 20 Form; Status: 25 Under revision*) The IMPETUS platform/tools should help problem solving by suggesting actions to consider and offering alternative suggestions.	
Adaptability enables "user-IMPETUS platform team" to recognize and adapt fluidly to unexpected characteristics of a situation. The IMPETUS platform should have multiple options to recognize an unexpected situation and address it.	
Source: WP1 (human machine teaming), WP7 (user validation)	**Dependencies**:
Importance: 02 Required CPAD important - likely, similar to other ones	**Feasibility**:

# 38 (*Category:* *Technology integration; Type: 20 Form; Status: 25 Under revision*) The IMPETUS platform/tools should be able to let the user control (stop or override) its processes.	
Calibrated Trust is supported when the user has a strong understanding of when and how much to trust the IMPETUS platform in context. The user should understand clearly when the IMPETUS platform can be relied on, when more oversight is needed, and when performance is unacceptable. To help the user calibrate trust, the IMPETUS platform can provide information sources, and the credibility of those sources.	
Source: WP1 (human machine teaming), WP7 (user validation)	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - likely, similar to other ones	**Feasibility**:

# 39 (*Category:* *Technology integration; Type: 20 Form; Status: 25 Under revision*) The IMPETUS platform/tools should be clear about it's trustworthiness/confidence level so users can determine how much and when to trust it.	

<table>
<tr><td colspan="2">Achieving Common Ground means that pertinent beliefs, assumptions, and intentions are shared among team members. Common Ground is constantly and actively updated and maintained so that team members (both user and IMPETUS platform) can maintain a shared picture of what’s happening in the world and engage in backup behavior to support each other.

Added on 09/04:
All predictions, suggestions or otherwise processed information (based on collected data) presented to the user should be accompanied by a level of certainty (e.g. accuracy of a ML algorithm's prediction), on which the user can base it's judgment whether to trust the presented information.</td></tr>
<tr><td><b>Source</b>: WP1 (human machine teaming), WP7 (user validation)</td><td><b>Dependencies</b>:</td></tr>
<tr><td><b>Importance</b>: 02 Required
CPAD
important - likely, similar to other ones</td><td><b>Feasibility</b>:</td></tr>
</table>

<table>
<tr><td colspan="2"><b># 40 (<i>Category:</i></b> <i>Technology integration;</i> <b><i>Type:</i></b> <i>20 Form;</i> <b><i>Status</i></b>: <i>25 Under revision</i><b>)</b>
The IMPETUS platform/tools should update their assumptions to support the user.</td></tr>
<tr><td colspan="2">This requirement captures published recommendations on how to present information to support simplicity and understandability. The user should be able to view and interact with information in order to understand the implications of the data.</td></tr>
<tr><td><b>Source</b>: WP1 (human machine teaming), WP7 (user validation)</td><td><b>Dependencies</b>:</td></tr>
<tr><td><b>Importance</b>: 02 Required
CPAD
the platform will be easy to be used for the end users. This means that we have to consider some rework after the first implemetation: we will collect feedbacks form the users during some "hands on" sessions.
We have also to consider training sessions + a manual or a video-tutorial to let the end user to learn and revise</td><td><b>Feasibility</b>:
The rationale deals with understndability of the output (of the system) to the user, but the requirement mentions elicitation of assumptions underlying the generation of this output (i.e. how this output was computed). I'd advise to split this requirement into 2.</td></tr>
</table>

<table>
<tr><td colspan="2"><b># 41 (<i>Category:</i></b> <i>Technology integration;</i> <b><i>Type:</i></b> <i>20 Form;</i> <b><i>Status</i></b>: <i>25 Under revision</i><b>)</b>
The IMPETUS platform should be easy to use for a variety of final users.</td></tr>
<tr><td colspan="2">front end ergonomics development must have the same priority of the back end "engine": the final users, after a proper training, have to gain time in their operative duties. If they will lose only a second comparing with their current timing, Impetus will fail</td></tr>
<tr><td><b>Source</b>: End-user perspective</td><td><b>Dependencies</b>:</td></tr>
<tr><td><b>Importance</b>: 01 Deal breaker
CPAD
very important- likely similar to other ones</td><td><b>Feasibility</b>:</td></tr>
</table>

<table>
<tr><td><b># 42 (<i>Category:</i></b> <i>Technology integration;</i> <b><i>Type:</i></b> <i>20 Form;</i> <b><i>Status</i></b>: <i>25 Under revision</i><b>)</b>
IMPETUS platform should have 2 different interfaces, one for physical events SOC operators, another for cybersecurity SOC operators.</td></tr>
<tr><td>Data collected from CCTVs, sensors and all the other sources, could be stored in the same data lake/data center</td></tr>
</table>

(to be effectively managed and protected). 2 dashboard - interconnected maybe - could take and show these data according to the final users' responsibility (in particular, SOC operators involved in "physical" events management and SOC operators involved in cybersecurity duties)	
Source: End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - 2 different UIs, one for SOC operators and the other for IT-services people are required. the 2 UIs could be "derived" from one unique "root" combining different widgets	**Feasibility**:

# 43 (*Category:* *Technology integration;* *Type:* *20 Form;* *Status*: *25 Under revision*) The platform interface should allow end-users to configure which tools they want to use at a given time, depending on their operational needs.	
Final users must have the possibility to activate one or more tools in the same moment, according to the general situation they are monitoring. Likely there will be tools always running (e.g. the tools able to detect something)	
Source: End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - Likely similar to other ones	**Feasibility**:

# 44 (*Category:* *Technology integration;* *Type:* *20 Form;* *Status*: *25 Under revision*) When something suspicious or alarming is detected, the platform interface should provide an alert that effectively grabs the attention of the operators.	
the alert must claim the attention of the operators (e.g. a pop up blinking, with a sound, etc.). When the operator opens the alert message, IMPETUS platform must provide all the relevant information: type of emergency, where, how many people involved, etc. If something has been detected by a CCTV or sensor, the platform must open the involved CCTV(s) to show what is going on. If the alert is a cybersecurity alarm, the platform must provide a description of the attack and the best solution (if any)	
Source: End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - Otherwise the platform is useless	**Feasibility**:

# 45 (*Category:* *Technology integration;* *Type:* *20 Form;* *Status*: *25 Under revision*) The user interface (including graphical elements) should be available in multiple languages, including the language(s) preferred locally by end-users.	
The user interface must be readily and unequivocally understood by the end-user.	
Source: End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD very important, also in terms of dissemination and	**Feasibility**:

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

further adoption	

# 46 (*Category:* *Smart City Data; Type:* *20 Form; Status*: *25 Under revision*) The change detector should raise an alert when sensor data do not follow an expected behavior, according to historical data for any variable under observation	
IMPETUS can notify different users when it catches a particular phenomenon that could be described via the change in data distribution of any combination of variables under observation. The variables describe physical observations (e.g. PM2.5, CO2, pedestrian traffic, temperature...)	
Source: WP4, T4.1, D1.2 section 2 (intelligent layer)	**Dependencies**:
Importance: 02 Required CPAD this could be a matter of the end-user's way to visualize information coming from collected data	**Feasibility**:

# 47 (*Category:* *Smart City Data; Type:* *20 Form; Status*: *25 Under revision*) The event classifier should raise an alert when sensor data represents a previously defined class of threat	
IMPETUS should notify different users when it identifies a dangerous situation from the data, according to the description of the possible classes of situations provided by the cities	
Source: WP4, T4.1, D1.2 section 2 (intelligent layer)	**Dependencies**:
Importance: 01 Deal breaker CPAD very important	**Feasibility**:

# 48 (*Category:* *Technology integration; Type:* *10 Functional; Status*: *25 Under revision*) The IMPETUS platform/tools should provide the choice betwen multiple levels of automation to best support operators in recognizing and adapting to unexpected situations.	
Adaptability enables operators to recognize and adapt fluidly to unexpected characteristics of a situation. Autonomy should have multiple options to recognize an unexpected situation and change course, or suggest course changes, to address evolving, dynamic situations.	
Source: WP1 (human machine teaming), WP7 (user validation)	**Dependencies**:
Importance: 02 Required CPAD important and useful	**Feasibility**:

# 49 (*Category:* *Technology integration; Type:* *10 Functional; Status*: *25 Under revision*) The IMPETUS platform should be a modular platform where the individual tools can be added or removed without negating the functionality of the platform as a whole.	
The modularity of the platform allows for implementation in a diverse set of cities. Different cities have different visions and operational needs, and IMPETUS should be able to cater to most of them.	

<table>
<tr><td><b>Source</b>: End-user perspective</td><td><b>Dependencies</b>: Related to #43</td></tr>
<tr><td><b>Importance</b>: 01 Deal breaker
CPAD
very important - we agree tha this is a deal breaker. Also for dissemination and future adoption</td><td><b>Feasibility</b>:</td></tr>
</table>

<table>
<tr><td colspan="2"><b># 50 (<i>Category:</i></b> <i>Technology integration;</i> <b><i>Type:</i></b> <i>30 Targeted use;</i> <b><i>Status</i></b><i>: 25 Under revision</i><b>)</b>
The IMPETUS platform should be able to provide access rights for end users based on roles, responsibilities and operational needs.</td></tr>
<tr><td colspan="2">Platform owners must be able to tailor stakeholder access to the platform based on operational needs. Adaptable access levels is also a critical component in maintaining operational security.
For example: Different user groups have different rights to access and modify something (only the tech admin will be able to make significant changes) and to interact with the platform (e.g. supervisors could like to see some statistics of aggregated info in addition or alternatively to the view of the operators)</td></tr>
<tr><td><b>Source</b>: End-user perspective</td><td><b>Dependencies</b>:</td></tr>
<tr><td><b>Importance</b>: 01 Deal breaker
CPAD
important - other requirements are similar to this. Right?</td><td><b>Feasibility</b>:</td></tr>
</table>

<table>
<tr><td colspan="2"><b># 51 (<i>Category:</i></b> <i>Technology integration;</i> <b><i>Type:</i></b> <i>10 Functional;</i> <b><i>Status</i></b><i>: 25 Under revision</i><b>)</b>
Platform owners and operators should be able to filter, aggregate, compile (specific) data into formats which can be easily forwarded to other users from organisations which are not part of the IMPETUS operating environment.</td></tr>
<tr><td colspan="2">Operational circumstances may necessitate the sharing of data from the IMPETUS platform to users from external organisations. It should be possible to filter, aggregate, compile data into formats which allow for exports to these external user groups.</td></tr>
<tr><td><b>Source</b>: End-user perspective</td><td><b>Dependencies</b>:</td></tr>
<tr><td><b>Importance</b>: 02 Required
CPAD
important - could the information coming from the platform be "downloadable" in a cvs/xls file?</td><td><b>Feasibility</b>:</td></tr>
</table>

<table>
<tr><td colspan="2"><b># 52 (<i>Category:</i></b> <i>Technology integration;</i> <b><i>Type:</i></b> <i>10 Functional;</i> <b><i>Status</i></b><i>: 25 Under revision</i><b>)</b>
The public safety platform must integrate different capabilities for public safety</td></tr>
<tr><td colspan="2">This the main purpose of the platform. This is a very important characteristic of this project: although the selected technologies have been used in other domains, their combination within this project will go beyond the state of the art as the technologies represent already leading-edge developments in their fields and will be combined for the first time in the smart city domain.</td></tr>
<tr><td><b>Source</b>: DoA</td><td><b>Dependencies</b>:</td></tr>
<tr><td><b>Importance</b>: 02 Required
CPAD
important - even if the term "integrate" should be better</td><td><b>Feasibility</b>:</td></tr>
</table>

detailed. If the idea is that the platform should allow the end-user to use different tools (and their different capabilites) within one unique "place", we agree. We could also think to an integration of (a part of) the tools, but this could be dangerous: what could happen if one tool will be removed?	

# 53 (*Category:* *Technology integration;* *Type:* *10 Functional;* *Status*: *25 Under revision*) The platform should provide a secure access to the specific tools from the integrated view.	
Every partner is expected to have a functional and working tool. Within the platform, the user can access to every tool and use it independently from the others.	
Source:	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - has this req the same meaning of #52 or it is the exact opposite?	**Feasibility**:

# 54 (*Category:* *Technology integration;* *Type:* *30 Targeted use;* *Status*: *25 Under revision*) The IMPETUS platform should allow the connection of simoultaneous users.	
Cities have expressed the necesity of having access to the platform from different institutions and users.	
Source: End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD vey important	**Feasibility**:

# 55 (*Category:* *Technology integration;* *Type:* *10 Functional;* *Status*: *25 Under revision*) The platform should allow for logging of "false alarms".	
False alarms during operations can not be excluded. It may be useful for future improvements and as statistical records to log false alarms occurrences detected by the platform.	
Source: D1.2 section 2	**Dependencies**:
Importance: 02 Required CPAD it is not a deal breaker but we consider it very important and useful for further developments	**Feasibility**:

56 (*Category:* *Technology integration;* *Type:* *30 Targeted use;* *Status*: *25 Under revision*) Smart cites should have immediate cross organizational communications channels that are known, interoperable and of suffient bandwidth to account for surge capacity.
Lessons learned from multiple events show that all involved organizations must be able to communicate among the participants and that the network must have surge capacity

Source: Open data sources, documented in D1.2 section 2.3.2.2	**Dependencies**:
Importance: 03 Nice-to-have CPAD important - but maybe it is to be considered a "strong advice" for the cities regarding their operative processes.	**Feasibility**:

# 57 (*Category: Operations; Type: 10 Functional; Status: 25 Under revision*) Smart cites should develop a methodology to utilize CCTV sources and ensure their effective use, including related to technical and social aspects	
Lessons learned from multiple cities show impacts on CCTV results from poor training in areas such as image aspect, ethnicity of target population and data analytics	
Source: Open data sources, documented in D1.2 section 3	**Dependencies**:
Importance: 02 Required CPAD important - this req refers to the ethical framework. Even if this req sounds more like a "strong advice", the Cosortium should find a way to allow the use of the IMPETUS platform only to those cities which already have a video-surveillance regulation and refer to GDPR or similar set of rules	**Feasibility**:

# 58 (*Category: Smart City Data; Type: 40 Development; Status: 25 Under revision*) The Access Control methodology and the ingestion process must use standard interfaces.	
Support the communication with other parties. Access control methodology and ingestion process can work at different points including the overall platform and tools. Each specific tool could have its own access control methodology and ingestion process. Simplified Description: Traditional requirement to ease the integration between different components using standard APIs	
Source: DoA	**Dependencies**:
Importance: 02 Required CPAD important: the use of API is strongly "advocated"	**Feasibility**:

# 59 (*Category: Technological capabilities; Type: 30 Targeted use; Status: 25 Under revision*) Results from AI should always be monitored by humans before leading to action.	
"Human-in-the-loop"; maintaining a "healthy sceptisism" to the existing capabilities of artificial intelligence".	
Source: WP1, D1.2: operational challenges (section 5)	**Dependencies**:
Importance: 01 Deal breaker CPAD very important	**Feasibility**:

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

# 60 (*Category:* *Smart City Data; Type: 30 Targeted use; Status: 25 Under revision*) The platform operators should manage Access Control policies.	
Operators can i) define access control policies driving access control methodology and ii) drive access to data to support the cybersecurity processes in the platform. Simplified Description: Traditional Access control requirement saying that operator can manage rights to access data and that this can be used in order to evaluate the cybersecurity of the platform itself.	
Source: DoA	**Dependencies**:
Importance: 02 Required CPAD important - BUT only "admin" operators should be able to define access control policies, so NOT all the end-users!	**Feasibility**:

# 61 (*Category:* *Smart City Data; Type: 10 Functional; Status: 25 Under revision*) The ingestion process should support ingestion of structured and unstructured data.	
Support the ingestion of different sources of data measured and collected by the pilot cities. Sources are heterogeneous and can both involve structured and unstructured data. Simplified Description: It refers to different structure of the data. Technically speaking they have to be managed differently this is why we mention them.	
Source: DoA; WP4	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - the platform must be able to handle with different types of data (with different structures)	**Feasibility**:

# 62 (*Category:* *Smart City Data; Type: 10 Functional; Status: 25 Under revision*) Data analytics should be executed on ingested data.	
Support the execution of the analytics on the ingested data. Ingested data are the source of analytics supporting the decision process taken by the platform operators using the tools. Simplified Description: This is just to say that the data we are using for analytics are the ones ingested in the platform by the ingestion procedure and not any data. It is “should” meaning that we are not saying that we will not use external data one day.	
Source: DoA	**Dependencies**:
Importance: 02 Required CPAD important - having clear which data are used but not limiting further different data ingestion processes	**Feasibility**:

63 (*Category:* *Smart City Data; Type: 10 Functional; Status: 25 Under revision*)

The Ingestion process must support standard ingestion workflows on data measured and collected by the pilot cities.	
Support different types of ingestion of data (e.g., batch, micro-batch, stream) measured and collected by the pilot cities. Simplified Description: This to say that we can ingest data from cities via streaming (any APIs offered by the tools allowing streaming) or via batches (files)	
Source: DoA; WP4	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - using standard workflows or standard procedures to ingest data both via streaming or batches will make easier any further adoption of the platform (e.g. by other cities)	**Feasibility**:

# 68 (*Category:* *Technological capabilities;* *Type:* *40 Development;* *Status*: *25 Under revision*) Relevant sensor data should be provided by the smart cities to properly train AI/ML-based tools.	
To make the anonzmiyed weapon detection (AWD) tool work in both partner cities environments we need CCTV footage of the cameras that will be used for the detection in both partner cities. Not having this is like not having gas for a engine. This is a MUST.	
Source: Solution provider need	**Dependencies**:
Importance: 01 Deal breaker To make the AWD tool work in both partner cities we need CCTV footage from the cameras that will be used as input for the AWD tool. That footage has to have two versions: 1) One version with people without any weapons 2) One version with epople holding weapons in their hands The footage has to becaptured using an 8MP CCTV cameras (true 4K, 8 frames per seconds), using the camera night mode setting also known as IR (Infra Red) and not to be confuded with thermal imaging. The footage needed is 30min at dawn, 30 min after dawn, 30min at the brightest hours, 30 min at sunset, 30min at night. The footage has to be captured during a sunny day, a rainy day, a snowy day. The footage must include people with and without drawn weapons such as small magazine fedhand gun and asault rifles (AR 15 or M16 or what was used in the 2011 mass shooting). When looking at the captured video footage, the human unaided eye must be able to recognize the weapon that are entering the camera field angle of view. CPAD very important - we understand and agree.	**Feasibility**: 03 Easy This shoudl be a very easy task, yet due to the limitation of workforce in both partner cities due to Covid-19, it is very challenging to produce.

69 (*Category:* *Technological capabilities;* *Type:* *40 Development;* *Status*: *25 Under revision*)

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

Alerts from tools should be tested and developed in accordance with systems and protocols in place in the smart cities.	
When the AWD is in Red Alert mode, it shares alerts in near real-time. We need to know what type of protocols we can use to share these alerts. Is it GPRS? Do we send the alerts to the VMS (Video Management System) ? If yes which VMS is in place ? Which version ? Who do we contact so we can do remote tests?	
Source: Solution provider need	**Dependencies**: This requirement becomes more or less important/relevant depending on the how/whether other(s) are implemented.
Importance: 01 Deal breaker This is a must task. yet we simply need to know ahead of time how we can share our alerts with the relevant teams in the partner cities. CPAD very important - the alerts should be provided within the platform UI	**Feasibility**: 03 Easy This is a fairly easy task. It is just time consuming.

# 70 (*Category:* *Technological capabilities; Type: 40 Development; Status: 25 Under revision*) Sensors should be made available (potentially installed) in the smart cities to support the use of the individual tools.	
E.g., without CCTV cameras, we cannot use the AWD tool.	
Source: Solution provider need	**Dependencies**:
Importance: 01 Deal breaker We have been discussing with both partner cities and we must have CCTV cameras installed for both use cases that are respectively: 1) Oslo City Hall, outdoor. 2) Piazza Dei Signori, outdoor CPAD very important - we agree. We are running (more like a turtle than a rabbit) to install new-generation Avigilon CCTVs in Piazza dei Signori	**Feasibility**: 01 Difficult

# 71 (*Category:* *Technological capabilities; Type: 30 Targeted use; Status: 25 Under revision*) The implementation of edge devices should conform to their recommended range of utilisation and avoid increasing vulnerabilities.	
To run the AWD we will use edge devices that will need to be stored in a place away from the public and in an environment that will not exceed 30 degrees celcius.	
Source: Solution provider need	**Dependencies**:
Importance: 02 Required This requirements is crucial for the AWD tool to work as inferencing edge devices cannot be stored in over heating areas. CPAD	**Feasibility**: 02 Doable

important - we have to better understand where the right place for edge devices is (what are they?). But new CCTVs will be installed in a building belonging the municipality: I guess there the temperature is never higher than 30°C because of the air conditioning system	

# 73 (*Category:* *Technological capabilities; Type: 40 Development; Status: 25 Under revision*) The cyber integrity of tools and their components should be ensured before their integration in the platform.	
The cyber integrity of tools and their components SHOULD be ensured before delivery to be used in the public.	
Source:	**Dependencies**: VPN, SSH Key
Importance: 01 Deal breaker If we leave this out, the AWD tool will be hacked sooner or later. Our Jr. Data Scientist came up with a very good solution which will require us to put the edge devices that will be used for the AWD tool on our own VPN so that no one but Cinedit and the Oslo team can access the edge devices that will process the CCTV that are to be installed. CPAD important - we have to talk about this topic. Of course the AWD tool must be protected. I guess it won't be "reachable" from the internet, it will work within an internal - not accessible net.	**Feasibility**: 01 Difficult Requires good communication with the person relevant in the partner city so we can set uyp our VPN (Virtual Private Network). Overall, since the world started to do remote work due to Covid-19, all companies are using VPN's so that their task force can work from home. We will do the same.

# 74 (*Category:* *Technology integration; Type: 30 Targeted use; Status: 25 Under revision*) The platform should support operations during all phases of the intelligence cycle.	
The intelligence cycle includes: planning and direction, collection, processing, analysis and dissemination. The motivation for the requirement is that the platform will be especially useful for analysts/operators if all of the phases are taken into account when developing the platform. This means that less external tools will have to be used to support the process. In addition to collection and analysis that are obvious features of the platform, it will be useful if the platform also will include communication features for team members (planning and direction) and dissemination (for example reports that can easily be compiled within the platform). The requirements 74-78, 80 can be seen in relation as they are requirements addressing operational needs, mainly within intelligence.	
Source: WP1, D1.2: operational challenges (section 5)	**Dependencies**:
Importance: 02 Required CPAD important - the end users could use the platform - to improve security when planning an event - to detect dangerous or risky situations - to provide support to emergency-operators on the filed or citizens	**Feasibility**: 02 Doable

# 75 (*Category:* *Technological capabilities;* ***Type:*** *30 Targeted use;* ***Status***: *25 Under revision***)** The platform tools involving social media, dark web and cyber threat intelligence should allow for targeted intelligence collection.	
Where relevant, tools in the platform involving social media and cyber threat intelligence should support functions that allow the operators/analysts to select sources for collection according to specific and dynamic needs. The collection process can be customized to local conditions, local threat actors and local targets. There is a need for assessment by humans (operators/analysts) (See requirement #80). The requirements 74-78, 80 can be seen in relation as they are requirements addressing operational needs, mainly within intelligence.	
Source: WP1, D1.2: operational challenges (section 5)	**Dependencies**: Relates to #76
Importance: 02 Required The platform tools that include big data collection SHOULD allow for targeted intelligence collection CPAD important	**Feasibility**: 01 Difficult

# 76 (*Category:* *Technological capabilities;* ***Type:*** *10 Functional;* ***Status***: *25 Under revision***)** The IMPETUS tools should have analysis functions that enable the operators to filter and narrow down the information that is collected according to intelligence needs.	
The operators will need built-in analysis functions in order to find the relevant information from the collected data. The requirements 74-78, 80 can be seen in relation as they are requirements addressing operational needs, mainly within intelligence.	
Source: WP1, D1.2: operational challenges (section 5)	**Dependencies**: Relates to #75
Importance: 01 Deal breaker CPAD very important - we agree	**Feasibility**: 01 Difficult

# 77 (*Category:* *Operations;* ***Type:*** *30 Targeted use;* ***Status***: *25 Under revision***)** The platform should allow for efficient information sharing between operators from different intelligence disciplines.	
The platform must allow operators manning different tools within different intelligence disciplines of the platform, or safety actors situated at different SOCs to efficiently share information between them and especially in real time. The requirements 74-78, 80 can be seen in relation as they are requirements addressing operational needs, mainly within intelligence.	
Source: WP1, D1.2: operational challenges (section 5)	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - we agree. Likely, other reqs state	**Feasibility**: 01 Difficult

similar things	

# 78 (*Category:* *Smart City Data;* ***Type:*** *10 Functional;* ***Status****: 25 Under revision***)** The platform should support data and control flow integration.	
The advantage of having a fusion platform is the ability to combine information/data from multiple sources/tools. In order for this to be efficient, the operators have to be assisted in some way in combining the relevant information from different sources. This assistance could for instance be in form of alerts or notifications, or it could be a search mechanism allowing the operators to find relevant information from all the tools. Hence, "combining information/data" can mean something as simple as showing some data side by side; but it can also mean something that would make decisions based on details of the data. The platform supporting data and control flow integration does not necessarily mean that all tools need to make use of this possibility. This is essentially a high-level requirement that might need to be supported by multiple more detailed requirements in the future. The requirements 74-78, 80 can be seen in relation as they are requirements addressing operational needs, mainly within intelligence.	
Source: WP1, D1.2: operational challenges (section 5)	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - we agree	**Feasibility**: 01 Difficult

# 79 (*Category:* *Ethics;* ***Type:*** *10 Functional;* ***Status****: 25 Under revision***)** The IMPETUS platform should have well defined user roles to guarantee access to personal data only to authorised authorities and individuals.	
Personal data must be only available to authorised parties. It must be kept unavailable and classified for most of the platform users, and only some of the parties could eventually get access in case of an emergency or threat.	
Source:	**Dependencies**: Relates to #82
Importance: 01 Deal breaker CPAD very important - of course we have to guarantee that the platform is used only by authorized people (and authorized only for security reasons). The same for the collected data and related info	**Feasibility**: 02 Doable

# 80 (*Category:* *Operations;* ***Type:*** *30 Targeted use;* ***Status****: 25 Under revision***)** Performing or receiving threat assessments and mapping of threat actors and targets should be part of the routine for the operators of the platform.	
The platform cannot understand the societal, cultural and local context by itself. It must be guided by operators/analysts who will decide what to collect; and operators/analysts must have the societal, cultural and local context in mind when analysing the collection and detection results. Correct and timely threat assessments will be important for the operators ability to understand, interpret and assess the platform outputs.	

The requirements 74-78, 80 can be seen in relation as they are requirements addressing operational needs, mainly within intelligence.	
Source: WP1, D1.2: operational challenges (section 5)	**Dependencies**:
Importance: 01 Deal breaker CPAD very important. Likely, this req is similar to other ones	**Feasibility**: 01 Difficult

# 81 (*Category:* *Operations; Type: 10 Functional; Status: 25 Under revision*) Training plans should be created to prepare operators and first responders for using the platform during complex and stressful scenarios.	
(i.e., decision-making and response under uncertainty).	
Source: WP1, D1.2: operational challenges (section 5)	**Dependencies**:
Importance: 01 Deal breaker CPAD very important. IMPETUS is not only a plattform but also processes releted to	**Feasibility**: 01 Difficult

# 82 (*Category:* *Operations; Type: 10 Functional; Status: 25 Under revision*) Roles, tasks and responsibilities in the decision-making process should be defined clearly in the new concepts of operation.	
Decision-making roles and responsibilities should be clarified, i.e., who is responsible for combining the bits and pieces of information from the platform and make decisions based on that information.	
Source: WP1, D1.2: operational challenges (section 5)	**Dependencies**:
Importance: 01 Deal breaker CPAD very important. Likely, this req is similar to other ones	**Feasibility**: 01 Difficult

# 83 (*Category:* *Operations; Type: 10 Functional; Status: 25 Under revision*) Division of responsibilities should be defined clearly relative to the use of tools in the platform, including who is using which tool(s) based on authority and skillset.	
This has importance for the development of the platform and for the form of the platform, but also for the operations.	
Source: WP1, D1.2: operational challenges (section 5)	**Dependencies**:
Importance: 02 Required Mismatch: 'Should' and 'Deal Breaker'. 19.03.21: SINTEF. Importance updated. (Deal breaker is automatically filled in by default if no other level is chosen). The importance level is for the end users to choose. All requirements drafts should be written with SHOULD at this point. CPAD	**Feasibility**: 01 Difficult

important - responsabilities related to the tools have to be clear for everyone	

# 84 (*Category:* *Technological capabilities;* *Type:* *40 Development;* *Status*: *25 Under revision*) Design and development of the platform technologies should take into account human factors and capabilities.	
Avoid that technology is developed based on technological terms alone. This has importance both for form and development.	
Source: WP1, D1.2: operational risks (section 5)	**Dependencies**:
Importance: 02 Required This reads like a project (Impetus) requirement. By default, this is what Impetus set out to do, considering the user and Ethics. That is why I do not see the need/ sense to include this in this list. SINTEF 19.03.21: rephrased to enhance clarity. CPAD important - I agree to the comment here above. I move to "Required" the level of importance but likely this req is included in the project definition	**Feasibility**: 01 Difficult

# 86 (*Category:* *Technology integration;* *Type:* *30 Targeted use;* *Status*: *25 Under revision*) The IMPETUS platform should be intended to always be in operation	
Data should be collected and processed h24. At least "to feed" those tools based on big-data management and AI. But a "red button" to stop all activities related to data processing should be considered. Instead, turning off te UI should be always possible.	
Source: End-user perspective	**Dependencies**:
Importance: 02 Required CPAD important - anyway, likely, a deeper analysis related to this topic should be undertaken	**Feasibility**: 01 Difficult "difficult" is default value - still to be evaluated

# 87 (*Category:* *Technology integration;* *Type:* *30 Targeted use;* *Status*: *25 Under revision*) The Impetus platform should not be modified by the operative end-users	
Concept of vertical organisation of the end-users. End-users should get different alarms and information depending on their role and should be able to interact in different ways with the platform. The operative end-users, meaning for Padova those who work in the SOC and in the IT service office of the Municipality, should only have access to the info provided by the platform, not change the settings. Access to the settings should be prerogative of higher level personnel.	
Source: End-user perspective	**Dependencies**: Related to #89
Importance: 01 Deal breaker	**Feasibility**: 01 Difficult

CPAD very important - this req is similar to other ones	"difficult" is default value - still to be evaluated

# 88 (*Category:* *Technological capabilities;* ***Type:*** *10 Functional;* ***Status****: 25 Under revision***)** The IMPETUS platform should include detection and alerts of suspicious content from social media.	
Since one of the tool is the SMD, we would like to get an alert if worrying contents are detected. Worrying or suspicious content is determined by operational needs, in a given context.	
Source: DoA; End-user perspective	**Dependencies**:
Importance: 02 Required CPAD interesting - e.g. counting negative comments untill their number is higher than a treshold could provide an alert related to people "sentiment" and suggest a deeper anaysis	**Feasibility**: 01 Difficult INS: Inskit Spotlight/SMD does not count with a processing module for an alerting system. We would need to read a detailed rationale in this requirement to assess the feasibility of it. A first thought, based only on the requirement title, is that this requirement will imply developments in a higher level layer (since SMD will not be able to produce and/or provide alerts by itself).

# 89 (*Category:* *Technology integration;* ***Type:*** *30 Targeted use;* ***Status****: 25 Under revision***)** The platform administrator should be able to integrate tools and to configure the interface (e.g, visualizations).	
Concept of vertical organisation of the end-users. Access to the settings (and so interface visualization/configuraration) should be prerogative of higher level personnel, as the possibility to add new tools and the integration with them	
Source: End-user perspective	**Dependencies**: Related to #87
Importance: 02 Required CPAD important - likely similar to other ones	**Feasibility**: 01 Difficult "difficult" is default value. Still to be evaluated

# 90 (*Category:* *Technology integration;* ***Type:*** *10 Functional;* ***Status****: 25 Under revision***)** The Impetus platform inputs-outputs should be customised according to the specificities of the cities (not only the pilot ones)	
Since the basic idea is to develop a similar platform even in other eu cities (not only the project partner cities), we must consider that every city has a different infrastructure and different needs. So the platform should adapt to the specificities of various eu cities.	
Source: DoA; End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - this for future adoptions (by other cities)	**Feasibility**: 01 Difficult "difficult" is default value. Still to be evaluated

91 (*Category:* *Technology integration;* ***Type:*** *30 Targeted use;* ***Status****: 25 Under revision***)**

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

The Impetus platform should be supplemented with a detailed user manual (usage and ordinary maintenance).	
Since the city staff should be able to use the platform properly and to manage some problems that may occur, a manual would be very helpful. On the other hand, we think teaching lessons would be difficult to undertake, for language and distance reasons.	
Source: DoA; End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - both for a "smooth" implementation and for future adoptions (by other cities)	**Feasibility**: 01 Difficult "difficult" is default value. Still to be evaluated

# 92 (*Category:* *Technological capabilities;* *Type:* *10 Functional;* *Status*: *25 Under revision*) In the case of security events, the Impetus platform should provide the possibility to alert the population of an emergency situation (e.g., via text messaging or other channel).	
We would like to develop this funcionality related to the PTRO. Padova is thinking of an sms alert system, while Oslo of using an app already existing called TRIO.	
Source: End-user perspective	**Dependencies**:
Importance: 03 Nice-to-have Not promised in the DoA, but interesting and relevant capability, maybe related to other capacity to generate reports to external users and collaborators CPAD before cancelling this req, please let's talk about it. Maybe we can develop something "propedeutical"	**Feasibility**: 01 Difficult Who would make the developments to fulfil the requirement? Who can judge the feasability? Yes you are right. Canceled. CPAD before cancelling this req, please let's talk about it. Maybe we can develop something "propedeutical"

# 93 (*Category:* *Cyber;* *Type:* *10 Functional;* *Status*: *25 Under revision*) The IMPETUS platform must be protected from outside intruders.	
It is very important to guarentee the citizens privacy and the operation of the platform. We don't want anybody to steel information or to interfere with the police nor the IT city system work.	
Source: DoA; End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD very important	**Feasibility**: 01 Difficult "difficult" is default value. Still to be evaluated

# 94 (*Category:* *Operations;* *Type:* *30 Targeted use;* *Status*: *25 Under revision*) Information generated from the IMPETUS platform should be accessible from different emergency services and operational stations.	
Concept of horizontal organisation. Not only the local police SOC, but even other SOCS, should have access to the platform output, since different bodies work together in the security/emergency/first aid field and should be aligned.	
Source: End-user perspective	**Dependencies**:

Importance: 01 Deal breaker CPAD very important - likely, this req is similar to other ones	**Feasibility**: 01 Difficult "difficult" is defaut value - Still to be evalauted

# 95 (*Category:* *Technology integration; Type: 10 Functional; Status: 25 Under revision*) The Impetus modules must be easy to integrate with other tools if needed	
In the future the cities may want to add new tools or change the one already existing and should be able to do it	
Source: DoA; End-user perspective	**Dependencies**:
Importance: 02 Required CPAD important - likely, similar to other ones	**Feasibility**: 01 Difficult "difficult" is default value. Still to be evaluated

# 96 (*Category:* *Technological capabilities; Type: 10 Functional; Status: 25 Under revision*) The IMPETUS platform should be open to receive input from city officials/emergency personnel to integrate the information received by sensors/data	
Since the platform may miss something and may not provide all the info by it-self, it would be of great help if it could receive input by the officials/emergency staff, in order to make a better picture of the running situation. These info may be insert manually of with some automatic funcionality,tbd.	
Source: End-user perspective	**Dependencies**:
Importance: 03 Nice-to-have CPAD interesting - will be possible to broadcast adding info to other SOCS via IMPETUS platform?	**Feasibility**: 01 Difficult "difficult" is default value. Still to be evaluated

# 97 (*Category:* *Technology integration; Type: 10 Functional; Status: 25 Under revision*) The IMPETUS platform must remain a standalone platform but should be able to interact with existing devices and platforms in the cities.	
A stand alone platform is better to avoid integration with the cities system(that are not possible both for Padova and Oslo) and to facilitate the scalability of the platform in other Eu cities that may have the same issue. However, to make the platform more efficient, it should be able to interact with the cities tools/platform. So yes interaction, no integration	
Source: End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD very important -we have to develop a stand alone platform ready to collect data from a data lake provided by the city (so the platform has to be able to connect to it)	**Feasibility**: 01 Difficult "difficult" is default value - Still to be evaluated

# 98 (*Category:* *Technology integration; Type: 20 Form; Status: 25 Under revision*) The IMPETUS platform should provide alerts for different operators within the same organisation or	

emergency service.	
somehow related to req. 27 and 54. In this case we want to underline the general rule.	
Source: End-user perspective	**Dependencies**:
Importance: 02 Required CPAD important - likely, similar to other ones	**Feasibility**: 01 Difficult "difficult" is default value - Still to be evaluated

# 99 (*Category:* *Technology integration;* *Type:* *20 Form;* *Status*: *25 Under revision*) The IMPETUS platform should provide alerts for different operators across different organisations.	
Related to req 42, but this is more on a generic level	
Source: End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - likely, similar to other ones	**Feasibility**: 01 Difficult "difficult" is default value - Still to be evaluated

# 100 (*Category:* *Smart City Data;* *Type:* *20 Form;* *Status*: *25 Under revision*) The IMPETUS platform should provide aggregated data and diagrams to allow for strategic monitoring and planning.	
The main goal is to have statistics and aggregated data in order to make strategic analysis.	
Source: End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - likely, similar to other ones	**Feasibility**: 01 Difficult "difficult" is default value - Still to be evaluated

# 101 (*Category:* *Smart City Data;* *Type:* *20 Form;* *Status*: *25 Under revision*) The IMPETUS platform should support users in creating personalized aggregated data and diagrams to perform specific analyses.	
The main goal is to have statisticas and aggregated data in order to make startegic analysis	
Source: End-user perspective	**Dependencies**:
Importance: 01 Deal breaker CPAD very important. Likely, similar to other ones	**Feasibility**: 01 Difficult "difficult" is default value - Still to be evaluated

# 102 (*Category:* *Operations;* *Type:* *30 Targeted use;* *Status*: *25 Under revision*) The platform should allow for efficient and coordinated information sharing between SOC operators and responders in the field in a purposeful format in order to increase situational awareness for first responders.	
The platform with all its integrated tools will be able to contribute with valuable information that the SOC operators will have to communicate to responders in the field (police, fire fighters, ambulance personnel and	

others). In order for this information to increase situational awareness it needs to be transferred in a manner that is efficient and in real time. It also needs to be in a format that is easily and quickly understood. (e.g. visualisation instead of long pieces of text). The advantage of the integrated platform is also that first responders can receive coordinated information from several tools simultaneously.	
Source: D1.1; D1.2, Section 5	**Dependencies**:
Importance: 01 Deal breaker CPAD very important - we agree	**Feasibility**: 01 Difficult "difficult" is default value - Still to be evaluated

# 103 (*Category:* *Technology integration;* *Type:* *30 Targeted use;* *Status*: *25 Under revision*) The platform should allow for logging and saving of findings in such a manner that it can be used as legal evidence in court.	
The platform will during its activities detect and find information that will later be valuable as evidence. It is important for the SOC operators to be able to save this documentation in an organized and secure manner. It can for example be saved in folders/or cases related to certain events, investigations or certain crime clusters. This documentation might later have to be used in court as evidence. It is therefore important that the logging/saving abide by GDPR and other local and international frameworks for data protection, data security and data privacy.	
Source: D1.1; D1.2, Section 5	**Dependencies**:
Importance: 02 Required CPAD important - we agree	**Feasibility**: 01 Difficult "difficult" is default value - Still to be evaluated

# 104 (*Category:* *Operations;* *Type:* *10 Functional;* *Status*: *10 Draft*) The IMPETUS project must develop new concepts of operation and implementation guidelines to support the use of new technological capabilities in operations.	
New capabilities provided by the different tools will impact the way operations are conducted. New concepts of operation need to take into account the transformation brought about by the new technological capabilities and means of support offered by the platform.	
Source: DoA	**Dependencies**:
Importance: 01 Deal breaker	**Feasibility**: 01 Difficult

# 105 (*Category:* *Cyber;* *Type:* *10 Functional;* *Status*: *10 Draft*) The IMPETUS project must develop a cybersecurity framework to support Smart Cities in addressing cyber security issues associated with technology for safety.	
Source: DoA	**Dependencies**:
Importance: 01 Deal breaker From DoA	**Feasibility**: 01 Difficult

106 (*Category:* *Cyber;* *Type:* *10 Functional;* *Status*: *10 Draft*)

The cyber security framework should include a security awareness training.	
Need to increase the security-awareness training amongst smart city personnel.	
Source: DoA	**Dependencies**:
Importance: 01 Deal breaker	**Feasibility**: 01 Difficult

Members of the IMPETUS consortium

	SINTEF, Strindvegen 4, Trondheim, Norway, https://www.sintef.no	Joe Gorman joe.gorman@sintef.no
	Institut Mines Telecom, 19 place Marguerite Perey, 91120 Palaiseau, France, https://www.imt.fr	Joaquin Garcia-Alfaro joaquin.garcia_alfaro@telecom-sudparis.eu
	Université de Nimes, Rue du Docteur Georges Salan CS 13019 30021 Nîmes Cedex 1, France, https://www.unimes.fr	Axelle Cadiere axelle.cadiere@unimes.fr
	Consorzio Interuniversitario Nazionale per l'Informatica, Via Ariosto, 25, 00185 – Roma, Italy, https://www.consorzio-cini.it	Donato Malerba donato.malerba@uniba.it
	University of Padova, Via 8 Febbraio, 2 - 35122 Padova, Italy, https://www.unipd.it	Giuseppe Maschio giuseppe.maschio@unipd.it
	Biotehnoloogia ja Meditsiini Ettevõtluse Arendamise Sihtasutus, Tiigi 61b, 50410 Tartu, Estonia, https://biopark.ee	Sven Parkel sven@biopark.ee
	SIMAVI, Complex Victoria Park, Corp C4, Etaj 2, Şos. Bucureşti – Ploieşti, nr. 73 – 81, Sector 1, Bucureşti, Romania, https://www.simavi.ro	Gabriel Nicola Gabriel.Nicola@simavi.ro Monica Florea Monica.Florea@simavi.ro
	Thales Nederland BV, Zuidelijke Havenweg 40, 7554 RR Hengelo, Netherlands, https://www.thalesgroup.com/en/countries/europe/netherlands	Johan de Heer johan.deheer@nl.thalesgroup.com
	Cinedit VA GmbH, Poststrasse 21, 8634 Hombrechtikon, Switzerland, https://www.cinedit.com	Joachim Levy j@cinedit.com

INSIKT INTELLIGENCE	Insikt Intelligence, Calle Huelva 106, 9-4, 08020 Barcelona, Spain, https://www.insiktintelligence.com	Dana Tantu dana@insiktintelligence.com
SIXGILL	Sixgill, Derech Menachem Begin 132 Azrieli Tower, Triangle Building, 42nd Floor, Tel Aviv, 6701101, Israel, https://www.cybersixgill.com	Benjamin Preminger benjamin@cybersixgill.com Ron Shamir ron@cybersixgill.com
XM CYBER	XM Cyber, Galgalei ha-Plada St 11, Herzliya, Israel https://www.xmcyber.com	Lior Barak lior.barak@xmcyber.com Menachem Shafran menachem.shafran@xmcyber.com
Comune di Padova	City of Padova, via del Municipio, 1 - 35122 Padova Italy, https://www.padovanet.it	Enrico Fiorentin fiorentine@comune.padova.it Stefano Baraldi Baraldis@comune.padova.it
Oslo	City of Oslo, Grensen 13, 0159 Oslo, Norway, https://www.oslo.kommune.no	Osman Ibrahim osman.ibrahim@ber.oslo.kommune.no
Institut za sigurnosne politike ISP	Institute for Security Policies, Kruge 9, 10000 Zagreb, Croatia, http://insigpol.hr	Krunoslav Katic krunoslav.katic@insigpol.hr
T S I M E	International Emergency Management Society, Rue Des Deux Eglises 39, 1000 Brussels, Belgium, https://www.tiems.info	K. Harald Drager khdrager@online.no
UniSMART Fondazione Università di Padova	Unismart – Fondazione Università degli Studi di Padova, Via VIII febbraio, 2 - 35122 Padova, Italy, https://www.unismart.it	Alberto Da Re alberto.dare@unismart.it