

Practitioners Guides

Using advanced technology raises ethical, data privacy, cybersecurity and operational issues

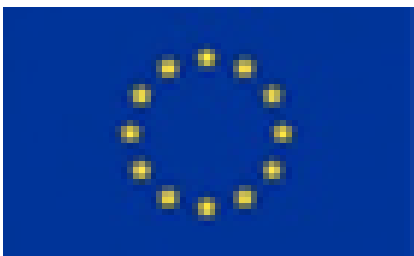
Advanced technological solutions to collect, analyse and use data in security operations offer great potential to improve safety in cities. But they cannot just be used “straight out of the box”: numerous issues related to ethics, data privacy, cybersecurity and operational practices must be addressed to enable successful deployment and long-term operational impact.

How the IMPETUS "Practitioners Guides" help

IMPETUS developed approaches to addressing these issues, and learned many valuable lessons along the way. The Practitioners Guides raise awareness and bring lessons learned in IMPETUS to a wider audience. They consist of guidelines, tutorial materials, checklists, reference information and more, covering three core areas:

- **Ethics:** how to integrate ethical principles and procedures respecting data privacy in operations
- **Cybersecurity:** how to guard against, detect and deal with cyber security risks in Smart City contexts
- **Operations:** how to integrate new technologies into existing working practices to enhance operations

The work presented here was carried out in the IMPETUS project. The project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883286.



1. Cover page	1
1.1 Front page	2
1.2 What are the Practitioners Guides	3
1.3 Practitioners Guides on Ethics & Privacy	3
1.3.1 Introduction and Readers Guide: Ethics & Privacy	5
1.3.2 Regulations and Standards	11
1.3.2.1 Relevant EU Regulations	11
1.3.2.2 Privacy Framework	14
1.3.3 Ethical and Data Privacy Issues	15
1.3.3.1 Ethical and Legal Issues	15
1.3.3.2 Privacy Issues	18
1.3.4 Ethical and Privacy Countermeasures	21
1.3.4.1 Recommendations on Ethical Issues	21
1.3.4.2 Privacy Enhancing Techniques for Smart Cities	24
1.3.4.2.1 User-side Techniques	25
1.3.4.2.2 Server-side Techniques	25
1.3.4.2.3 Communication Techniques	26
1.3.4.3 Case Study: LEx Ethical and Privacy Considerations	26
1.3.5 Ethical and Privacy Assessments of IMPETUS	27
1.3.5.1 Privacy Impact Assessments and Ethical Analysis	28
1.3.5.2 Experiences and Lessons Learnt - Ethical and Privacy Enforcement for Future Development	37
1.3.6 Further Reading and Standards	40
1.4 Practitioners Guide on Cybersecurity	42
1.4.1 Introduction and Readers Guide: Cybersecurity	44
1.4.2 Cybersecurity: Quick Intro	52
1.4.3 Principles of Cybersecurity	53
1.4.4 Social Considerations	58
1.4.5 Managing Cybersecurity: Quick Intro	59
1.4.6 Cybersecurity for Smart Cities	59
1.4.7 Cybersecurity Crisis Management	66
1.4.8 Context for Future Adaptation	71
1.4.9 Regulations Related to Cybersecurity	74
1.4.10 Cybersecurity Library	76
1.4.11 Cybersecurity Checklist for Smart Cities	78
1.5 Practitioners Guide on Operations	78
1.5.1 Introduction and readers guide: Operations	79
1.5.2 Description of Tools (and Platform)	81
1.5.2.1 Main Functions of (IMPETUS) Tools	81
1.5.2.2 Technical Information on (IMPETUS) tools	81
1.5.3 Impact on Operational SOC Processes	83
1.5.3.1 Direct Benefit from IMPETUS Tools	83
1.5.3.2 Impact on Basic Security Operations Center (SOC) Processes	85
1.5.3.3 Transformative Effects on Basic SOC Processes	85
1.5.3.4 Strategic Leverage for Improved Performance of the SOC as a Whole	86
1.5.4 Operational Challenges and Constraints	88
1.5.4.1 Potential Operator Overloads	89
1.5.4.2 Gains and Brittleness in Joint Attention, Awareness and Sensemaking	89
1.5.4.3 Degraded Modes	90
1.5.5 Potentials for Enhanced Operation	90
1.5.5.1 Ensuring Robustness of SOC Operations	93
1.5.5.2 Building Resilience from Robustness	95
1.5.6 Experiences	97
1.5.6.1 Tools and Their Impact	97
1.5.6.2 Challenges and Constraints	97
1.5.6.3 Utilisation of Potential	98
1.6 Brief history of the Practitioners Guides	98
1.7 About IMPETUS	98
1.8 Copyright notice	99

Front page

What are the Practitioners Guides?

How do I navigate the Practitioners Guides?

Practitioners Guide on Ethics & Privacy

Practitioners Guide on Cybersecurity

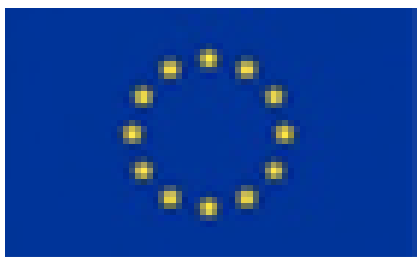
Practitioners Guide on Operations

About IMPETUS

Brief history of the Practitioners Guides

Copyright notice

The work presented here was carried out in the IMPETUS project. The project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883286.



What are the Practitioners Guides?

Who are the Practitioners Guides for?

The Practitioners Guides are aimed at a very wide readership: anyone with an interest in operational, strategic, ethical, legal, and data privacy issues in the context of using advanced technological solutions to collect, analyze and utilize data in security operations. The tools developed in our IMPETUS project are examples of the kind of advanced technologies we are considering – but the scope is wider than that, including (but not limited to) the use of algorithms, monitoring by electronic means, “Big Data” and “Internet of Things”.

Potential readers might include people with roles such as:

- Security Operations Center operator
- Security Operations Center supervisor
- IT personnel
- Intelligence Analysts
- Staff in local government with management and decision-making roles
- Policy makers
- Regular citizens
- Regulators
- Civil servants

The list is not exhaustive.

Why would I want to Make Use of the Practitioners Guides?

Based on the very wide readership, different parts of the Practitioners Guides will be relevant to some readers but not to others. We have adopted a modular approach where readers can easily browse to find the material relevant to their role.

The types of things you can learn about include:

- The general ethical, legal, and data privacy issues that you ought to be aware of if you want to deploy technology such as that developed in IMPETUS in security operations;
- Some particular issues that may apply depending on the specific functionality provided by a given tool;
- The overall advantages, opportunities, and challenges of using advanced technologies such as IMPETUS.

If you are already using, or considering adopting, some or all IMPETUS technologies you will also:

- Find practical guidance and support materials that will help you ensure compliance with relevant principles and regulations;
- Learn how new tools can be integrated into the IMPETUS platform and how the alerts and output from the platform can be integrated with existing infrastructure in the operator/owner's organization.

Relationship to the tools and platform developed in the IMPETUS project

The Practitioners Guides are *not* intended as a sales channel / marketing aid for the software developed in the project (tools + integrating platform).

Experience in developing and using the software was an important *input* to development of the Practitioners Guides.

The only “sales” aspect of the Practitioners Guides is to help sell the *overall idea* of using advanced technology to improve public safety: to help persuade potential adopters of such technology that concerns related to ethical, legal, cybersecurity and operational concerns can be addressed effectively. IMPETUS results are an *example* of the type of technologies under consideration: but there are others, and we are confident that new ones will emerge in future.

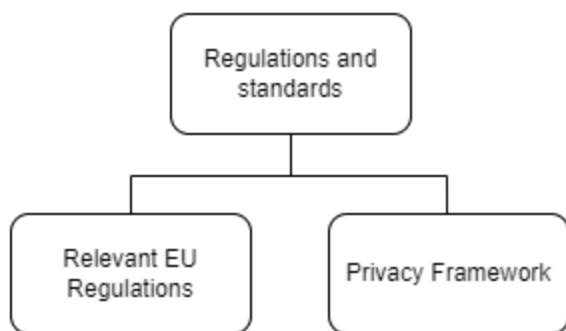


This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

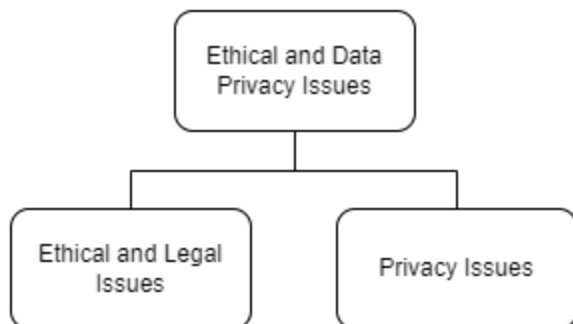
Copyright © The Impetus Consortium

Introduction and Readers Guide: Ethics & Privacy

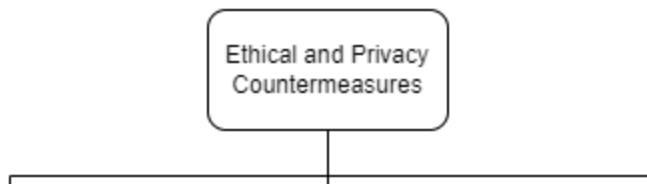
How are ethics and privacy protected by law?



What are the most common issues faced by the use of Smart City technology?



What are the concrete countermeasures to ethical and privacy issues?

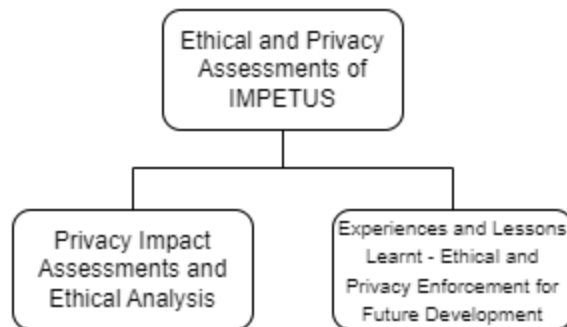


Recommendations on
Ethical Issues

Privacy Enhancing
Technologies for
Smart Cities

Case Study: LEx
Ethical and Privacy
Considerations

How prone is your tool to ethical and privacy issues?




Where can we find additional information?

Further Reading and
Standards

Introduction and Readers Guide: Ethics & Privacy

This Practionners Guide (PG) sets out general guidance on data privacy, data protection and data ethics concerning the use of big data, collected in the context of a smart city for the purposes of strengthening operational implementation of IMPETUS tools and advanced technologies, in general, to ensure safety and security in urban spaces.

 The PG on ethics and privacy is designed to:

- Establish common principles to support the operational and ethical use of data in the context of a smart city;
- Serve as a data risk-management tool taking into account fundamental human rights; and
- Set principles for obtaining, retention, use and quality control for data in the context of a smart city.

The data revolution was recognized as an enabler of the operational security and safety in urban spaces, not only to monitor progress but also to inclusively engage stakeholders at all levels to advance evidence-based policies. At the same time, there are legitimate concerns regarding risks associated with handling and processing of big data, particularly in light of the current regulatory landscape and in the absence of a common set of principles on data privacy, ethics and protection.

These concerns continue to complicate efforts to develop standardized and scalable approaches to data risk management in the context of smart cities. A coordinated approach is required to ensure the emergence of frameworks for privacy-preserving and responsible use of big data to ensure safety in public spaces.

Reaffirming that the right to privacy is a fundamental human right and recognizing the social value of data, this document aims to provide a harmonized general framework for accountable, adequately transparent, and responsible data handling practices across the different stakeholders, illustrated through IMPETUS use cases and developed tools.



This Practitioners Guide is not a legal document. It provides only a minimum basis for self-regulation, and therefore may be expanded and elaborated on by the implementing organizations of IMPETUS tools and platform.

Acknowledging the potential risks and harms as well as the benefits that can result from the use of big data, this document goes beyond individual privacy and considers potential effects on group(s) of individuals. Additionally, this PG takes into consideration standards of moral and ethical conduct, and recognizes the importance of different contexts. While mainly based on IMPETUS use cases, the PG on ethics and privacy may be expanded on and elaborated in the future, based on experiences and suggestions from readers.

For an open reading experience, the root page of the [Practitioners Guide on Ethics and Privacy](#) can be accessed and explored as desired.

The reading paths below offer suggestions for specific audiences, to ease their orientation within the set of materials related to ethics and privacy and in correspondence with other subjects approached by the Practitioners Guides. The refined reading suggestions are built mainly for:

Data Protection Officers	Users of security solutions (for example IMPETUS Users)
SOC Operators	
IT Security Personnel	
Intelligence Analysts	
Other Users	
Government Staff	General Users
Decision Makers	
Policy Makers	
Regulators	
Regular Citizens	

The "IMPETUS users" category addresses the personnel that work in the IMPETUS context.

The "General users" category addresses any other readers concerned of ethics and privacy aspects in relation to Smart City contexts.

Reading suggestions for Data Protection Officers

#reading_order	Section/ Chapter
1	Regulations and Standards
	Ethical and Data Privacy Issues
2	<ul style="list-style-type: none"> Ethical and Legal Issues
3 (optional)	<ul style="list-style-type: none"> Privacy Issues
	Ethical and Privacy Countermeasures
4	<ul style="list-style-type: none"> Recommendations to Ethical Issues
5 (optional)	<ul style="list-style-type: none"> Privacy Enhancing Technologies for Smart Cities
6	<ul style="list-style-type: none"> Case Study- LEx Ethical and Privacy Considerations
	Ethical and Privacy Assessments of IMPETUS
7	<ul style="list-style-type: none"> Privacy Impact Assessments and Ethical Analysis

8 (optional)	<ul style="list-style-type: none"> • Experiences and Lessons Learnt - Ethical and Privacy Enforcement for Future Development
9	<i>How to conduct an effective DPIA</i>
10	<i>How to deal with workers' monitoring?</i>
11 (optional)	<i>How to deal with Big Data analytics?</i>
12 (optional)	<i>What considerations should be fulfilled by social media analysis tools?</i>
13 (optional)	Further readings and standards

Reading suggestions for SOC Operators

#reading_order	Section/ Chapter
1 (optional)	Ethical and Data Privacy Issues
2 (optional)	Ethical and Privacy Countermeasures
	Ethical and Privacy Assessments of IMPETUS
3	<ul style="list-style-type: none"> • Privacy Impact Assessments and Ethical Analysis
4 (optional)	<ul style="list-style-type: none"> • Experiences and Lessons Learnt - Ethical and Privacy Enforcement for Future Development
5 (optional)	<i>How to conduct an effective DPIA</i>
6	<i>How to deal with workers' monitoring?</i>
7 (optional)	<i>How to deal with Big Data analytics?</i>
8 (optional)	<i>What considerations should be fulfilled by social media analysis tools?</i>
9 (optional)	Further readings and standards

Reading suggestions for IT Security Personnel

#reading_order	Section/ Chapter
1 (optional)	Regulations and Standards
	Ethical and Data Privacy Issues
2 (optional)	<ul style="list-style-type: none"> • Ethical and Legal Issues
3	<ul style="list-style-type: none"> • Privacy Issues
4 (optional)	<ul style="list-style-type: none"> • Recommendations to Ethical Issues
5	<ul style="list-style-type: none"> • Privacy Enhancing Technologies for Smart Cities
6	<i>Server-side Techniques</i>
7	<i>Communication Techniques</i>
8	<ul style="list-style-type: none"> • Case Study- LEx Ethical and Privacy Considerations
	Ethical and Privacy Assessments of IMPETUS
9	<ul style="list-style-type: none"> • Privacy Impact Assessments and Ethical Analysis
10 (optional)	<ul style="list-style-type: none"> • Experiences and Lessons Learnt - Ethical and Privacy Enforcement for Future Development
11 (optional)	Further readings and standards

Reading suggestions for Intelligence Analysts

#reading_order	Section/ Chapter
1 (optional)	Regulations and Standards
2 (optional)	Ethical and Data Privacy Issues
	Ethical and Privacy Countermeasures
4 (optional)	<ul style="list-style-type: none"> Recommendations to Ethical Issues
	<ul style="list-style-type: none"> Privacy Enhancing Technologies for Smart Cities
5	<i>Server-side Techniques</i>
	Ethical and Privacy Assessments of IMPETUS
6 (optional)	<ul style="list-style-type: none"> Privacy Impact Assessments and Ethical Analysis
	<ul style="list-style-type: none"> Experiences and Lessons Learnt - Ethical and Privacy Enforcement for Future Development
7	<i>How to deal with Big Data analytics?</i>
8	<i>What considerations should be fulfilled by social media analysis tools?</i>
9 (optional)	Further readings and standards

Reading suggestions for other IMPETUS Users

#reading_order	Section/ Chapter
1 (optional)	Regulations and Standards
	Ethical and Data Privacy Issues
2	<ul style="list-style-type: none"> Ethical and Legal Issues
3	<ul style="list-style-type: none"> Privacy Issues
	Ethical and Privacy Countermeasures
4	<ul style="list-style-type: none"> Recommendations to Ethical Issues
5 (optional)	<ul style="list-style-type: none"> Privacy Enhancing Technologies for Smart Cities
6	<ul style="list-style-type: none"> Case Study- LEx Ethical and Privacy Considerations
	Ethical and Privacy Assessments of IMPETUS
7 (optional)	<ul style="list-style-type: none"> Privacy Impact Assessments and Ethical Analysis
	<ul style="list-style-type: none"> Experiences and Lessons Learnt - Ethical and Privacy Enforcement for Future Development
8	<i>How to conduct an effective DPIA</i>
9 (optional)	<i>How to deal with workers' monitoring?</i>
10	<i>How to deal with Big Data analytics?</i>
11	<i>What considerations should be fulfilled by social media analysis tools?</i>
12 (optional)	Further readings and standards

Reading suggestions for Government Staff

#reading_order	Section/ Chapter
1 (optional)	Regulations and Standards

	Ethical and Data Privacy Issues
2	<ul style="list-style-type: none"> • Ethical and Legal Issues
3 (optional)	<ul style="list-style-type: none"> • Privacy Issues
	Ethical and Privacy Countermeasures
4	<ul style="list-style-type: none"> • Recommendations to Ethical Issues
5 (optional)	<ul style="list-style-type: none"> • Privacy Enhancing Technologies for Smart Cities
6	<ul style="list-style-type: none"> • Case Study- LEx Ethical and Privacy Considerations
	Ethical and Privacy Assessments of IMPETUS
7 (optional)	<ul style="list-style-type: none"> • Privacy Impact Assessments and Ethical Analysis
8	<ul style="list-style-type: none"> • Experiences and Lessons Learnt - Ethical and Privacy Enforcement for Future Development
9 (optional)	Further readings and standards

Reading suggestions for Decision Makers

#reading_order	Section/ Chapter
1 (optional)	Regulations and Standards
	Ethical and Data Privacy Issues
2	<ul style="list-style-type: none"> • Ethical and Legal Issues
3 (optional)	<ul style="list-style-type: none"> • Privacy Issues
	Ethical and Privacy Countermeasures
4	<ul style="list-style-type: none"> • Recommendations to Ethical Issues
5 (optional)	<ul style="list-style-type: none"> • Privacy Enhancing Technologies for Smart Cities
6	<ul style="list-style-type: none"> • Case Study- LEx Ethical and Privacy Considerations
	Ethical and Privacy Assessments of IMPETUS
7 (optional)	<ul style="list-style-type: none"> • Privacy Impact Assessments and Ethical Analysis
8	<ul style="list-style-type: none"> • Experiences and Lessons Learnt - Ethical and Privacy Enforcement for Future Development
9 (optional)	Further readings and standards

Reading suggestions for Policy Makers

#reading_order	Section/ Chapter
1	Regulations and Standards
	Ethical and Data Privacy Issues
2	<ul style="list-style-type: none"> • Ethical and Legal Issues
3 (optional)	<ul style="list-style-type: none"> • Privacy Issues
	Ethical and Privacy Countermeasures
4	<ul style="list-style-type: none"> • Recommendations to Ethical Issues

5 (optional)	<ul style="list-style-type: none"> Privacy Enhancing Technologies for Smart Cities
6	<ul style="list-style-type: none"> Case Study- LEx Ethical and Privacy Considerations
	Ethical and Privacy Assessments of IMPETUS
7 (optional)	<ul style="list-style-type: none"> Privacy Impact Assessments and Ethical Analysis
8	<ul style="list-style-type: none"> Experiences and Lesssons Learnt - Ethical and Privacy Enforcement for Future Development
9 (optional)	Further readings and standards

Reading suggestions for Regulators

#reading_order	Section/ Chapter
1	Regulations and Standards
	Ethical and Data Privacy Issues
2	<ul style="list-style-type: none"> Ethical and Legal Issues
3 (optional)	<ul style="list-style-type: none"> Privacy Issues
	Ethical and Privacy Countermeasures
4	<ul style="list-style-type: none"> Recommendations to Ethical Issues
5 (optional)	<ul style="list-style-type: none"> Privacy Enhancing Technologies for Smart Cities
6	<ul style="list-style-type: none"> Case Study- LEx Ethical and Privacy Considerations
	Ethical and Privacy Assessments of IMPETUS
7 (optional)	<ul style="list-style-type: none"> Privacy Impact Assessments and Ethical Analysis
8	<ul style="list-style-type: none"> Experiences and Lesssons Learnt - Ethical and Privacy Enforcement for Future Development
9 (optional)	Further readings and standards

Reading suggestions for Regular Citizens

#reading_order	Section/ Chapter
1 (optional)	Regulations and Standards
	Ethical and Data Privacy Issues
2	<ul style="list-style-type: none"> Ethical and Legal Issues
3 (optional)	<ul style="list-style-type: none"> Privacy Issues
	Ethical and Privacy Countermeasures
4	<ul style="list-style-type: none"> Recommendations to Ethical Issues
5 (optional)	<ul style="list-style-type: none"> Case Study- LEx Ethical and Privacy Considerations
	Ethical and Privacy Assessments of IMPETUS
6 (optional)	<ul style="list-style-type: none"> Privacy Impact Assessments and Ethical Analysis
	<ul style="list-style-type: none"> Experiences and Lesssons Learnt - Ethical and Privacy Enforcement for Future Development
7	<i>What considerations should be fulfilled by social media analysis tools?</i>

8 (optional)	Further readings and standards
--------------	--

Reading suggestions for General Users

#reading_order	Section/ Chapter
1	Regulations and Standards
	Ethical and Data Privacy Issues
2	<ul style="list-style-type: none"> Ethical and Legal Issues
3 (optional)	<ul style="list-style-type: none"> Privacy Issues
	Ethical and Privacy Countermeasures
4	<ul style="list-style-type: none"> Recommendations to Ethical Issues
5 (optional)	<ul style="list-style-type: none"> Privacy Enhancing Technologies for Smart Cities
6	<ul style="list-style-type: none"> Case Study- LEx Ethical and Privacy Considerations
	Ethical and Privacy Assessments of IMPETUS
7 (optional)	<ul style="list-style-type: none"> Privacy Impact Assessments and Ethical Analysis
8	<ul style="list-style-type: none"> Experiences and Lessons Learnt - Ethical and Privacy Enforcement for Future Development
8 (optional)	Further readings and standards

Regulations and Standards



This section provides a summary of legal guidelines and data privacy standards. These references need to be considered in order to comply with ethical recommendations for the use of big data and AI algorithms to enhance safety in urban spaces. The following references are relevant to both [general](#) and [IMPETUS](#) users.


It includes an introduction to:

- [Relevant EU regulations](#), including the General Data Protection Regulation (GDPR), and other relevant EU guidelines that need to be considered by tool providers and users, dealing with personal and sensitive data, that need to be examined with respect to the use of specific technologies or the context of different applications and involved actors.
- [Privacy framework](#), providing tool boxes to assess the level of data privacy protection with respect to implemented techniques and procedures.

General recommendation: As a result of [all basic legislation](#) and [relevant guidelines](#), it is recommended that all tools' providers and users of smart cities' technologies should consider the following keypoints:

1. *Clear identification of all involved stakeholders and their roles.*
2. *Clear identification and understanding of all technologies and tools to be used.*
3. *Identification and precise definition of the potential role of private actors concerning any form of data manipulation (collection, analysis, access, sharing, storage, deletion, and others).*
4. *Understanding and applying relevant legal norms for data collection and processing, emphasizing personal data protection, with respect to local, European and international standards.*
5. *Clear definition of data utilization for public purposes.*
6. *Special consideration of machine learning and other types of intelligent algorithms in data collection and processing, and the role and capacity of human operators when algorithms are being utilized.*

Relevant EU Regulations

 This page introduces EU legal and policy requirements, in the context of a smart city, namely for the usage of collected data by governmental entities and also the sharing of these data between different actors.

In order to illustrate the consideration of different texts, we point out their relevance and present general recommendations to the organizations implementing or aiming to implement IMPETUS and similar technologies in the context of a smart city.

Four main directives are identified and briefly introduced hereafter:

1. [General Data Protection Regulation \(GDPR\)](#)
2. [Law Enforcement Directive \(LED\)](#)
3. [Ethics Guidelines for Trustworthy AI](#)
4. [Proposal for the Artificial Intelligence Act](#)

1. General Data Protection Regulation (GDPR)

Title: *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 ([General Data Protection Regulation](#))*

Summary: The *GDPR* is a globally known and respected legislation offering high levels of protection regarding collecting and processing personal data. The Regulation is directly applicable in all Member States and offers a unified approach to protecting personal data in the European Union. Any data processor and controller who does not abide by the GDPR rules face severe penalties, such as €20 million or 4% of global revenue (whichever is higher), plus data subjects have the right to seek compensation for damages.

GDPR builds on the 1950 [European Convention on Human Rights](#) where it was stated that *everyone has the right to respect for his private and family life, his home and his correspondence*. As technology progressed (widespread of online banking from the 2000s, emergence of Facebook in 2006, growth of Google etc.), the EU recognized the need for modern protections and GDPR was put into effect on May 25, 2018.

The GDPR defines an array of **legal terms** such as:

Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. [Pseudonymous](#) data can also fall under the definition if it's relatively easy to identify someone from it.

Data processing is any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, and erasing.

Data subject is the person whose data is processed.


Data controller is the person who decides why and how personal data will be processed.

Data processor is a third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations. They could include cloud servers or email service providers.

The GDPR also enumerated a comprehensive list regarding data subjects' rights, e.g, the right to be informed, the right of access, the right to erasure, the right to restrict processing, *etc.*

If the data is being processed, it must be done according to these protection and accountability principles, and data gathered must be handled by implementing [appropriate technical and organizational measures](#).

Relevance to IMPETUS: The GDPR Regulation is relevant for IMPETUS tools and the platform that collect and analyze personal data for purposes other than those described under the [LED Directive section](#).

 When we use terms with capital letters, we refer to the definitions given by the GDPR and summarized hereabove.

Data Protection Officers (DPOs) are figures at the heart of the legal framework established by GDPR, facilitating many organisations in complying with its provisions. Under the GDPR, it is mandatory for certain Data controllers and processors to designate a DPO. Nevertheless, even when the GDPR does not specifically require the appointment of a DPO, organisations may sometimes find it useful to designate a DPO on a voluntary basis. Data Protection Officers must be appointed [in case of](#):

- public authority other than a court acting in a judicial capacity performing data processing,
- core activities requiring an entity to monitor people systematically and regularly on a large scale,
- core activities are large-scale processing of special categories of data or data relating to criminal convictions and offenses.

All users are nevertheless reminded to ensure that they have all relevant GDPR compliance protocols in place (for more information, please refer to this [link](#)).

2. Law Enforcement Directive (LED)

Title: [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

Summary: The so-called *Police Directive* or *LED* has been adopted in the same package as the GDPR and is effective from May 2018. Because the GDPR excludes its application in law enforcement bodies' criminal investigations and operations safeguarding against and preventing threats to public security, it became necessary to separately regulate the protection of personal data being processed in such circumstances. The LED adopts similar principles to protecting personal data as present in the GDPR, with some restrictive elements considering the particularities of criminal and public security threat investigations. [The Directive needs to be implemented in the Member State domestic law](#) by a specialized act which can differ to a certain extent from one Member state to another. Therefore, it is necessary to consult local legal experts when assessing the impact of the relevant national acts.

LED is not limited to processing by bodies who might be typically considered as '*law enforcement authorities*', but to any processing for law enforcement purposes, carried out by a public or private body who fits the definition of '*competent authority*' (such as local authorities when prosecuting litter fines, or local transport company in relation to ticket offences). This means that a potentially very large number and variety of bodies might fall under the scope, and the applicability of this regime needs to be assessed on a case-by-case basis.

Relevance to IMPETUS: The LED is relevant for all uses of IMPETUS tools and the platform that can be utilized in police (and related) investigations to tackle crime or threats to public security. Having in mind that, in principle, the law enforcement bodies are responsible for public security, each operation of personal data collection and subsequent analysis, sharing, storage, deletion, and others that are done to prevent public security threats or aid in criminal investigation, should be conducted under the auspices and control of a relevant law enforcement body (and, preferably, their personnel), with the security hub established by the partner city acting as a partner.

 In order to evaluate if a technology or service is within the scope of the LED, the following key questions should be considered:

- Is the body/entity in question a public authority, competent for law enforcement purposes?
- Is the body/entity in question any other body or entity authorized by law to exercise public authority and public powers for law enforcement purposes?
- Is the processing in question being carried out for the purposes of (a) the prevention of criminal offences, (b) the investigation of criminal offences, (c) the detection of criminal offences, (d) the prosecution of criminal offences or (e) the execution of criminal penalties?

Affirmative answers to these questions lead to potential subjectivity to LED. For example, given that the IMPETUS was designed to enhance the resilience of cities in the face of security threats in public spaces, it is recommended that all city users collaborate with local relevant law enforcement bodies. This should ensure that the police department assumes the principal role in all personal data manipulation activities conducted per the LED Directive and the relevant domestic law.

3. Ethics Guidelines for Trustworthy AI

Title: [Ethics Guidelines for Trustworthy AI](#), Independent High-Level Expert Group on Artificial Intelligence


Summary: The EU Ethics Guidelines for Trustworthy AI (EGTAI) is a set of recommendations for all artificial intelligence algorithms deployers to adhere to ensure the so-called "trustworthy artificial intelligence." According to the Guidelines, trustworthy AI should be:

- (1) **lawful** - respecting all applicable laws and regulations,
- (2) **ethical** - respecting ethical principles and values,
- (3) **robust** - both from a technical perspective while taking into account its social environment.

The Guidelines assess seven basic principles and develop a set of issues and checklists to consider when preparing to deploy such algorithms:

- *Human agency and oversight:* AI systems should empower human beings, allowing them to make informed decisions and fostering their fundamental rights. At the same time, proper oversight mechanisms need to be ensured, which can be achieved through human-in-the-loop, human-on-the-loop, and human-in-command approaches
- *Technical Robustness and safety:* AI systems need to be resilient and secure. They need to be safe, ensuring a fall back plan, as well as being accurate, reliable and reproducible.
- *Privacy and data governance:* besides ensuring full respect for privacy and data protection, adequate data governance mechanisms must also be ensured.
- *Transparency:* the data, system and AI business models should be transparent. Moreover, AI systems and their decisions should be explained in a manner adapted to the stakeholder concerned. Humans need to be aware that they are interacting with an AI system, and must be informed of the system's capabilities and limitations.
- *Diversity, non-discrimination and fairness:* Unfair bias must be avoided, as it could have multiple negative implications, from the marginalization of vulnerable groups, to the exacerbation of prejudice and discrimination.
- *Societal and environmental well-being:* AI systems should benefit all human beings, including future generations. It must hence be ensured that they are sustainable and environmentally friendly.
- *Accountability:* Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes.

Relevance to IMPETUS: As IMPETUS tools and the platform are mainly based on AI algorithms, the Guidelines have been designated as the core consideration for ethical recommendations that are relevant for all IMPETUS partners and deployers.

 All current/future users are recommended to assess a checklist introduced under the “[Ethics countermeasures](#)” and developed under the Ethics Guidelines consideration.


4. Proposal for the Artificial Intelligence Act

Title: *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence ([Artificial Intelligence Act](#)) and amending certain Union legislative acts*


Summary: The Draft Artificial Intelligence (AI) Act aims to become one of the first legislative instruments on a global scale regulating the use of different types of computer algorithms in various uses. The proposed Act builds on the risk-based approach applying different levels of requirements for different AI systems based on the potential risk they pose to fundamental rights of individuals, such as risks to the health and safety of individuals, respect for private life and protection of personal data, non-discrimination and equality between women and men. This has resulted in three categories of AI systems:

- **Prohibited AI practices:** These are AI systems that impose a substantial threat to the EU's values and fundamental rights. This includes practices that have a significant potential to manipulate a person through subliminal techniques beyond their consciousness or exploit specific vulnerable groups such as children or persons with disabilities in order to materially distort their behavior in a manner that is likely to cause them, or another person, psychological or physical harm.
- **AI systems which involve a *high risk*:** AI systems which constitute a high risk are allowed under the proposed Act but are strictly regulated. The classification as a high-risk AI system is based on the intended purpose of the system itself. And the proposed Act sets a list of legal requirements and obligations that should be considered by the AI system's sphere, e.g. importers, distributors and authorized representatives of the high-risk AI system.
- **AI systems which involve a *limited* or *minimal* risks:** These systems must be transparent to the human interacting with or being analyzed by the AI system. However, AI systems used for biometric categorization and deepfakes can be used without informing the recipient if the use is authorized by law to detect, prevent, investigate and prosecute criminal offenses.

Relevance to IMPETUS Platform: As it currently stands, the AI Act will impact the tools utilized by IMPETUS tools and the platform, especially when considering its application in police matters and public security at large. Detailed protocols and supervisory mechanisms must precisely regulate such tools. Advanced technologies, such as face recognition, will be permitted only in exceptional cases and with prior (or later) court (or other competent authority) approval.

 All users are advised to keep track of this legislative development.

Privacy Framework

 The privacy framework provides a procedural process and technical toolboxes that aim to help organizations identify and manage privacy risks, in order to build innovative products and services while protecting individuals' privacy, under specific regulations and legal contexts.

The privacy framework mainly highlights the importance of evaluating the privacy risks, through a Privacy Impact Assessment (PIA) (also called “Data Protection Impact Assessment”, in accordance with art. 35 GDPR) from the design phase of the product. A PIA consists of analysing how personal information are collected, used, shared, and maintained, in order to ensure main privacy properties.

This page will introduce the:

1. [privacy properties](#) that need to be fulfilled by designated products and services,
2. [PIA methodology](#) as detailed by European Union Agency for Cybersecurity (ENISA),
3. [use-case studies](#) as introduced by the [French data protection agency](#).

1- Privacy properties and general principles

The European Data Protection Board established main [Guidelines to give general guidance on the obligation of Data Protection by Design and by Default \(DPbDD\)](#), set forth in [Article 25 in the GDPR](#). DPbDD is an obligation for all controllers, irrespective of size and varying complexity of processing. And to be able to implement the requirements of DPbDD, it is crucial that the controller understands the data protection principles and the data subject's rights and freedoms.

In order to bridge the gap between the legal framework and the available technological implementation measures, the [European Union Agency for Cybersecurity \(ENISA\)](#) provides [an inventory of existing approaches, privacy design strategies, and technical building blocks of various degrees of maturity from research and development](#). Starting from the privacy principles of the legislation, important elements are presented as a first step towards a design process for privacy-friendly systems and services.

The main privacy properties that have to be enforced by the products and services dealing with personal and sensitive data in the context of a smart city, are summarized as follows:

- **Anonymity:** it means the ability of the user to access a resource or service without disclosing his identity to third parties. That is, the anonymity of a user means that he is not identifiable within a set of subjects, known as the anonymity set. Several levels of anonymity have been defined in the literature, ranging from complete anonymity (i.e., no one can reveal the identity of the user) to pseudo-anonymity (i.e., the identity is generally not known but can be disclosed if necessary) to pseudonymity (i.e., multiple virtual identities can be created and used in different settings).
- **Data minimization:** it is a fundamental feature of privacy preservation. It requires that service providers collect and process the minimum amount of information needed for appropriate execution of a service or a particular transaction. The goal is to minimize the amount of collected personal information by service providers, for instance, to reduce the risk of profiling and tracking users.
- **Unlinkability:** this property is essential for user privacy support and is closely related to the anonymity property. Unlinkability of two or more Items of Interest (Iols, e.g., users, messages, actions,) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these Iols are related or not.
- **Unobservability:** this property means the undetectability of a user against all users uninvolved in an IOI and its anonymity even against the other user(s) involved in that Iol. That is, a user can use a resource or a service, without being noticed by others. Unobservability also requires that third parties cannot determine if an operation is running.

2- Privacy Impact Assessment (PIA)

The European Union Agency for Cybersecurity (ENISA) provides a [risk data assessment methodology](#). It presents a [simplified approach](#) that can guide the Small and Medium Enterprises (SME)s through their specific data processing operation and help them evaluate the relevant security risks. This methodology could indeed be followed as first step also by other kinds of organizations, adding then some integrations and further evaluations, as needed. The ENISA's guidelines for SMEs propose an approach on evaluation of risk, which is based on four steps, as follows:

- the definition of the processing operation and its context.
- the understanding and evaluation of impact.
- the definition of possible threats and evaluation of their likelihood (threat occurrence probability).
- the evaluation of risk (combining threat occurrence probability and impact).

Following the evaluation of risk, the SMEs can adopt technical and organizational security measures (from a proposed list) that are appropriate to the level of risk, [as reported in the ENISA's guidelines](#).

3- Examples of Privacy Impact Assessments

ENISA initiative mainly relies on a detailed process provided by the [CNIL, the French data protection agency](#). It discusses a set of good practices aiming to address the privacy risks and impact on the protection of personal data a processing can result in, and provides a set of comprehensive guidelines with an illustrated use case to efficiently conduct this process, as follows:

- ☐ [Privacy Impact Assessment \(PIA\) : Application to connected objects](#)
- ☐ [Privacy Impact Assessment \(PIA\) 1 : Methodology](#)
- ☐ [Privacy Impact Assessment \(PIA\) 2 : Template](#)
- ☐ [Privacy Impact Assessment \(PIA\) 3 : Knowledge Basics](#)

Ethical and Data Privacy Issues

- The smart systems and smart technologies increase the risk of unethical use of personal and sensitive information. Having that in mind, in order to enhance the smart cities' resilience regarding security of public spaces, it is of utmost importance to identify and address ethical, legal and data privacy issues.

Ethical and data privacy issues are presented as follows:

1. [Ethical and legal issues](#)
2. [Data privacy issues](#)

We emphasize that the identified ethical and privacy issues are mainly focused on the smart cities' technological capabilities. Indeed, we consider the technological capacities of advanced AI algorithms to collect, transform, and share large amounts of data. ***The capacity to collect and handle "Big Data" presents a moral dilemma when faced with the need to protect citizens' privacy and personal data on one side of the spectrum (privacy in generalis) and protect citizens' livelihood and property from the other (public security).***

Therefore, a balance of the noted potentially conflicting interests should be established to simultaneously offer adequate and efficient mechanisms of preserving public security and personal privacy. Ethical issues arising out of the noted conflict of interests require constant study, vigilance, and practical considerations for all the involved stakeholders, but are not limited to the collection and processing of personal data.

Ethical and Legal Issues

☐ This page provides a summary of ethical and legal issues that need to be considered by both [IMPETUS](#) and [general users](#). These issues are mainly related to the use (collection, analysis, storage, access, and similar) of “Big Data” in security operations. This chapter is organised as follows:

1. [General context](#)
2. [Socio-technical environment](#)
3. [Involuntary data collection and manipulation](#)
4. [Moral machines](#)
5. [Stakeholders](#)

It is important to emphasize that the following analysis is tight the overall ecosystem, i.e., national and international regulations and guidelines, technical environments and involved actors, in the context of security and intelligence data-gathering operations.

1- General context

Smart systems aim at empowering human beings, allowing them to make informed decisions and fostering their fundamental rights, and at the same time, proper oversight mechanisms will be ensured using a human-in-the-loop approach. These technologies have to support human autonomy and decision-making, as prescribed by the principle of respect for human autonomy. They should act as enablers of a democratic, flourishing, and equitable society by supporting the user's agency, fostering fundamental rights and allowing for human oversight. Thus, a crucial component is to achieve Trustworthy AI which is tightly related to technical robustness, and closely linked to the principle of prevention of harm. This should also apply to potential changes in their operating environment or the presence of other agents (human and artificial) that may interact with the system in an adversarial manner.

From this perspective, and considering [relevant EU recommendations](#), it is of utmost importance to carefully identify the raised issues, associated with the context of usage.

2- Socio-technical environment

Whereas the public, in general, supports the primary efforts aimed at enhancing public security, the data-collection technology used in security operations may raise concerns about privacy preservation. 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 data processing. The ethical considerations revolve over the principal conflict of interests between collecting and analysing 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 as challenged by the civilizational strive to promote data rights as human rights (human-centric approach). As noted by the [European Commission \(EC\) in 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 analysis is to reconcile the two, at first glance, opposing forces, and to explore venues of co-existence (socio-technical environment), as represented in the table below.

Conflicting interests	
Security interests	Privacy interests
Necessity of identification	Right to anonymity
Access to data	Control of data and information symmetry
Arbitrary <i>post-hoc</i> information on data access	Informed access with consent
Storing and use of data for other purposes	Right to be forgotten
National and public security interests	Limitation of governmental surveillance
Right of secrecy	Right to redress
System of immunity and impunity	Responsibility and liability

Table 1: Conflicting interests

3- Involuntary data collection and manipulation

One of the most critical junctions in evaluating the ethical permissibility of data collection and manipulation concerns the instances of (semi-) automated involuntary data collection and manipulation activities. These activities include involuntary data collection (i.e., sensors, CCTV cameras, smart devices, ...), involuntary identification (i.e., face recognition, biometric data, automatic voice detection, ...), 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.

3.1- Mass surveillance

The all-out collection and manipulation of data are particularly pronounced in the differentiation between [targeted surveillance versus mass surveillance](#). Indeed, some IMPETUS tools may enable mass surveillance, considering that they are implementing AI algorithms.

i 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. At the same time, it is 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](#). 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](#)).

For concrete analysis of IMPETUS Tools, [please refer to the ethical analysis chapter](#).

3.2- Common goods

The common good principle should point to a particular value of general appreciation that gives justification for reducing other values, principles, and rights. Hereinafter, we will mainly focus on what the European Data Protection Supervisor (EDPS) referred to as the so-called [big data protection ecosystem](#), and therefore on the notions of privacy and personal data.

3.2.1- Privacy and personal data

The Convention for the Protection of Individual with regard to [Automatic Processing of Personal Data](#) (APPD) with its latest Protocol from 2018, recognizes the need to assess the protection of personal data, while considering the "... *diversification, intensification and globalization of data processing and personal data flows* ...". 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 fundamental rights' core echelon.

i The personal data implies any information pertaining to an identified or identifiable individual ([Art. 1. APPD](#); co-opted by the [General Data Protection Regulation](#)), irrespective of its nature. The term identifiable may relate to anonymized data that can be re-personalized.

The right of privacy is recognized as a universal human right by the [Universal Declaration of Human Rights](#). 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, particularly regarding the data protection defined by the [Charter of Fundamental Rights](#) of the EU (CRFUEU).

3.2.2- Limitation and exclusions

[CRFUEU 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, 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 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, including [the public interest and the exercise of official authority](#). 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. Based on GDPR (and other similar rules and other legal documents), national legislation usually adopts separate acts and statutes concerning the security and intelligence operations, criminal proceedings, public security issues, national security issues, 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](#). Indeed, most 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. On the European level, such matters are regulated by the [Directive \(EU\) 2016/680](#).

3.2.3- Traceable vs. untraceable data

The [GDPR](#) relates to the term pseudonymization, referring to a data management technique whereby a set of data relating 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.

4- Moral machines

One of the central ethical questions in the digital sphere (digital ethics, big data ethics) arising from the use of AI systems in data collection and manipulation (AI ethics) revolves around moral machines and [machine ethics concepts](#). These concepts evaluate the AI systems' ability to recognize morally significant situations, recognize relevant values, and factor those values into decisions they make.

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 Ethics Advisory Group 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.

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 (such as is the case with the [FD tool](#) in IMPETUS). The coding behind the noted system will allow designers (those who are designing the AI system) and deployers (those who are using an AI system or offering services through that AI system, also commonly referred to as controllers and processors) to delegate specific decision-making points to the AI system.

5- Stakeholders

It is important 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](#) for commercial purposes. Individuals whose data are 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.

Stakeholder	Role	Examples
Regulators	Regulate the implementation of security technology in public places	<ul style="list-style-type: none">• Policy makers at the city, national and European level
Decision-makers	Decide on investment in security technology solutions	<ul style="list-style-type: none">• City managers, smart city managers• National security agency managers• Critical infrastructure managers
Security actors	Use the technologies in security operations	<ul style="list-style-type: none">• Police and other security agencies• City, regional, national level• Operators and managers
Emergency actors	Interact with primary users in managing security events	<ul style="list-style-type: none">• Emergency agencies' actors• Critical infrastructure operators
Citizens	Residents of smart cities, impacted by the use of the technology	<ul style="list-style-type: none">• Citizens (including citizen groups)

Table 2: Stakeholders of Public Safety Solutions

Privacy Issues



This page introduces general data privacy concerns in the context of a smart city, presents the potential malicious entities and details specific data privacy issues associated with the different enabling technologies, as follows:

1. [Main privacy concerns](#)
2. [Threat models](#)
3. [Privacy issues](#)

1- Main privacy concerns

Below, a summary of the different concerns about data privacy, that should be considered and addressed, while implementing smart technologies in a large connected city:

- The first main concern is the widespread deployment of artificially intelligent processing algorithms that can be used in combination with the collected personal information to deduce involuntary correlations, leading to specific identification (other people, web pages, organizations, etc.).
- The second privacy concern is related to the tracking of spatial mobility, e.g., in relation to pedestrians, consumers and vehicles. Tracking is already a legitimate part of smart city technologies, as per ensuring safety in the public space, but there is a fear of misuse, e.g., related to unwanted surveillance.
- The third reported challenge consists of properly informing citizens about what the information is being used for, obtaining and maintaining informed consent in a practical manner. This challenge becomes even harder when combining different data sources. Indeed, aggregation of data may lead to profiling, discrimination, and political manipulation.
- The fourth concern consists of enforcing the requirement of processing personal data only within the European Union in accordance with art. 44 ff. of the [GDPR](#).



- There is a general concern from many cities on unnecessary or unwanted use of personal data for purposes such as marketing campaigns, telephone directory, contact-lists of some companies, etc. When it comes to personal data from video surveillance footage, the studies show a varying degree of concern from the citizens in different cities. Hence, we have to acknowledge that there are cultural differences between European countries on what is considered to be a privacy issue.

Taking the example of smart mobility, it is imperative that not only the privacy of the collected and analyzed data be preserved but also the running algorithms (usually considered as sensitive and proprietary). Regardless of the goal, the attacks and defenses relate to exposing or preventing the exposure of analysis algorithms (processes) and collected data.

2- Threat models

Data privacy risks are mainly related to environments, technologies and involved parties, and understanding privacy concerns, from a technical point of a view, leads to identify potential adversaries.

By adversaries, we refer to malicious actors that aim to gain access to personal data, while relying on:

-  data being transferred and processed that the adversary has access to,
-  and external knowledge of the adversary; e.g., information collected while colluding with other external malicious entities.

These adversaries may be passive or active, and considered under either semi-trusted or untrusted environments, presented as follows:

- Passive attacks: the adversary passively observes the data and performs inference or concludes connections, e.g., without changing anything in the process.
- Active attacks: the adversary actively changes the data or processes.

3- Privacy issues

In order to identify main privacy issues regarding the collection and processing of personal data, it is important to first understand main identifying features as detailed in the [GDPR](#).

Indeed, the data subjects are identifiable directly or indirectly. In directly approach, they can be identified using an identifier such as name or a national identification number. In an indirect approach, they can be identified using an online identifier or one of several special characteristics which expresses the physical, physiological, genetic, mental, commercial, or cultural identity of these natural persons. In the real world, identity information includes all data which are or can be assigned to a person in any context.

In a connected city, it is important to consider possibilities of remote monitoring using gathered personal information, and also assume that digital tools must be using information that is recorded, stored, and processed using either standalone sensors or devices around the physical location of the scenario. Based on these assumptions, here is a list of main identifiers and their category according to [GDPR](#).

Data identifier types	Identifiers
Ethnical origin	color of skin, language, traditional dress, tattoos, cast related markings.
Political & religious opinion	Protest/event banner, clothing, gesture, presence at historical event/dates, tattoos, speech
Genetic information	Physical access to protest or festival site may allow to collect genetic material such as used objects, food, etc.
Biometric information	Eyes, fingerprints, face, voice, birth marks, body shape, walking pattern.
Sexual orientation	Face (cosmetic and dress), voice (this could be an ethical issue, rather than privacy)
Health information	Temperature, smell (e.g., covid-19), waste-water samples, other vital signs
Online information	Mobile radio identities (Bluetooth/WiFi/NFC, 2G/3G/4G/5G), social media accounts, e-mail, vehicle number plate, IP address.

Considering the aforementioned identifiers, it is important to emphasize that privacy issues are tightly related to technologies (i.e., Internet of Things (IoT), Cloud and AI), that facilitate the sensing, collection and processing of these information. Main privacy exploits can be summarized as follows:

	<i>IoT</i>	<i>Cloud</i>	<i>AI</i>
Sensing layer	Data overcollection		<ul style="list-style-type: none"> • Data collection • Data poisoning • Backdoor injection
Collection layer	Lack of standardized secure short-band communication protocols		

Processing layer	Limited computation resources for advanced secure (cryptographic) algorithms	<ul style="list-style-type: none"> • Loss of data and computation control • Lack of knowledge about effective SLA enforcement • Multi-tenancy 	<ul style="list-style-type: none"> • Inference attacks • Model theft
Application layer	Open and insecure APIs		

In the following, we detail main issues related to each enforcing technology, namely [IoT-based challenges](#), [Cloud-based challenges](#) and [AI-based challenges](#).

IoT-based challenges

There are various privacy issues associated with smart devices that are mainly due to the massive data collection, focused on the sensing and communications layers. Indeed, the connected devices have the capability to be used as a mediator storage or a fog node to perform a small computation in the network. These sensing capabilities make them vulnerable end-points for collecting the exchanged data and enriching adversarial databases, thus conducting specific correlation and inference attacks.

While a huge number of applications are continuously proposed to provide various benefits for citizens, the majority of these applications gain access to private information *-without acquiring explicit informed consent-* and may transfer the collected data to *unauthorized* parties. Finally, the sensing capabilities of the smart devices *facilitate* the bypass of the data minimization, and most applications usually collect more data than the necessities of original functions, while in permission scope, which is known as data overcollection.

Cloud-based issues

To cope with the shortcomings of smart devices, i.e., processing and storage capacities, battery constraints, etc. various applications delegate the data and processing management to *external* cloud providers. In the following, we summarize common challenges raised by cloud infrastructures, platforms and applications.

- *Data and computation outsourcing*: by outsourcing the data to remote servers, data management is delegated to a third-party provider, usually considered as a semi-trusted or honest-but-curious entity. This raises privacy concerns, such as the anonymity of data owners.
- *Transfer of data outside the EU*: the lack of knowledge about the physical location of data in cloud services may have an impact on the data security, quality of services and might harm users' privacy. This latter is of utmost importance as data legislation regarding the collection and processing of data is different between different countries and regions, and can be more intrusive compared to the EU regulations.
- *Lack of knowledge about Service Level Agreements (SLAs)*: SLA is a contract signed between the client and the service provider including functional and non-functional requirements. It considers obligations, service pricing, and penalties in case of agreement violations. However, due to the abstract nature of clouds, SLA violations with regards to data involve data retention, privacy leakage.
- *Multitenancy*: this cloud feature means that the cloud infrastructure is shared and used by multiple users. In a nutshell, data belonging to different users may be located on the same physical machine, based on a specific resource allocation policy. Due to the multi-tenancy's economic efficiency, providers usually select this feature as an essential block for the cloud design. However, it generates new threats, such that, malicious users may exploit this co-residence issue to perform privacy (inference) attacks.

AI-based attacks

AI-based applications are key enablers of smart cities, empowering the extensive processing of gathered data and monitoring in real time the state of critical infrastructures. Unfortunately, they are generally considered as data-hungry tools and their benefits are often accompanied by a mostly black-box character and high complexity of the final algorithms in use, rendering conventional methods for safety assurance insufficient or inapplicable. As presented above, the massive collection of data from the different devices, a.k.a., referring to the sensing and data collection layers, constitute first threat vectors to attack intelligent systems due to their multitude and their limitations in terms of resources and security features. For example, by poisoning smart city's data, [adversaries](#) can try to fake the models, implying they will learn the correct correlation between data and the state of a critical system (modifying the model boundaries), or they can push the model in taking decisions that are hampering the city's infrastructure and population. It is clear that the strong link between sensor data and AI models, as well as the intrinsic weakness of the sensors themselves, introduce new risks that cannot be ignored, such as:

- *Backdoor injection*: it aims to mislead the AI model during the learning phase. In this case, the attacker crafts and distributes corrupted system's parameters in order influence the system behavior. The injected backdoors induce erroneous classification of inputs, with possibly disastrous consequences on the whole system's processes. Let us consider a AI model that is monitoring the quality of air pollution. An adversary can fake the model in believing that the presence of some chemicals in the air is innocuous, while they could be dangerous for the population.
- *Data Poisoning*: it aims to inject specific data, generally carefully selected, to fake an existing model into taking decisions that decrease performance and increase risks of the city's infrastructure and population. This category of attacks, called adversarial examples, builds on sensor inputs that can trick a deployed model, trained on benign data, into making a wrong decision. The most difficult aspect here is that adversarial example attacks are difficult to counteract since poisoned data are generally indistinguishable from a normal input for humans. For instance, let us consider a monitoring service in a smart city, via CCTV cameras. Adversarial examples can be used by an attacker interacting with different cameras to let the model believe that certain areas of the city are congested. This would force the model to reroute the traffic towards busy areas, as well as changing the traffic light timing, creating a gridlock. This would have disastrous consequences for instance in the case of a terrorist attack.
- *Model theft*: it is a mix of the previous two and is employed in scenarios, and mainly considered a security threat where ML models are either i) retrained over time or ii) alternative models have been trained and can be deployed on the basis of contextual information.
- *Inference attacks*: they include two main categories (a) inference about members of the population and (b) inference about members in the training set.

For the first case (a), an adversary can use the model's output to infer the values of sensitive attributes used as input to the model. Note that it may not be possible to prevent this if the model is based on statistical facts about the population: for example, suppose that training the model has uncovered a high correlation between a person's externally observable phenotype features and their genetic predisposition to a certain disease; this correlation is now a publicly known fact that allows anyone to infer information about the person's genome after observing that person.

For the second case (b), the focus is on the privacy of the individuals whose data was used to train the model. For instance, given a model and an exact data point, the adversary infers whether this point was used to train the model or not, and may also try to extract properties.

The following review paper, [appeared in the TIEMS annual conference, in 2021](#), details the privacy challenges in urban spaces, and identifies a set of recommendations to enhance the privacy by design concept, as highlighted by [EU regulations](#).

Proceedings of the TIEMS Annual Conference, December 2021, Paris, France

Privacy-preserving Challenges for Urban Safety

Nesrine Kaaniche Joaquín García-Alfaro

Telecom SudParis, Institut Mines-Télécom & Institut Polytechnique de Paris¹
kaaniche.nesrine@telecom-sudparis.eu, joaquin.garcia_alfaro@telecom-sudparis.eu

Abstract: We discuss privacy challenges for urban safety. We focus on privacy-preserving solutions that may allow urban safety operators to guarantee anonymous and unlinkable actions. We illustrate our analysis with the IMPETUS project scenarios and examine how design and architecture choices may impact compliance of personal data protection. Alternative designs that could lead to improvements in this matter are also briefly introduced.

Keywords: Privacy-preserving solutions, Privacy-Enhancing Technologies, Data Protection, Urban safety, Data Privacy Management.

1. Introduction

Multiple connected devices and sensors compose a smart city. These elements are connected through networks and their outputs are communicated to the inhabitants in an application via intelligent computing techniques. This relation between physical objects increases the possibility of turning cyber-attacks into physical attacks. On one hand, if urban safety is not secured, this means that essential services may fail. However, too excessive security measures can also lead to other problems, such as privacy violations [1]. On the other hand, urban safety is supported by the massive collection of data. Thus, privacy and security have to be carefully addressed, finding a proper balance between them [2].


In this paper, we explore and discuss some challenges to the development and implementation of public urban safety with regard to technological solutions in smart cities. Our focus is on privacy-preserving solutions, whose goal is to allow urban safety operators to guarantee anonymous and unlinkable actions, while maintaining an appropriate degree of security.

Through a case study based on the IMPETUS project [3], we examine some design and architecture choices, as well as how such decisions may affect compliance (e.g., technical and legal) of personal data protection. More specifically, we examine via the IMPETUS use case the problem of massive data collection, usually considered as the counter of emerging intelligent algorithms. Herein, we refer to Artificial Intelligence (AI). On one hand, the collection and manipulation of personal data raises alarming privacy issues; on the other hand, the learning algorithms, especially the most powerful ones, result in decision-making devices that are often not transparent and risk to be unfair. This refers to the privacy vs utility trade-off that has to be managed through the whole data life cycle.

We will focus on the different Privacy Enhancing Technologies (PET) to enforce the privacy by design principle. We examine the effectiveness of such mechanisms that has been studied and demonstrated by researchers and with various pilot implementations. However, they are still not well perceived by many operators mainly because they are reported to have an impact on the utility. This paper contributes to bridging the gap between the legal framework and the available technological implementation measures by providing an inventory of existing approaches and privacy design strategies of various degrees of maturity from research and development, from a service provider side. Starting from the privacy principles of the legislation, important elements are presented as a first step towards a design process

¹ 19 place Marguerite Perrey, 91120 Palaiseau, France.

Ethical and Privacy Countermeasures

 This section provides a set of recommendations to ethical issues and introduces a panorama of main technical mechanisms, generally known as Privacy Enhancing Technologies (PET), to be implemented in order to satisfy privacy requirements and comply with legislation, e.g., General Data Protection Regulation (GDPR).

It also illustrates different countermeasures through a real-world use case: it defines the ethical considerations and data privacy measures that have been implemented by IMPETUS while conducting Live Exercises (LEx). LEx are conducted to evaluate the applicability and effectiveness of the various tools during operations.

The section is organised as follows:

1. [Recommendations on ethical issues](#)
2. [Privacy Enhancing Technologies for smart cities](#)
3. [Case study: LEx ethical and privacy considerations](#)

Recommendations on Ethical Issues

In line with the Assessment List as prepared under [the Ethics Guidelines for Trustworthy AI](#), and having in mind the particularities of IMPETUS, this section provides preliminary checklists that serve as a starting point of legal and non-legal compliance with EU Guidelines for Trustworthy AI.

i All users are recommended to assess a checklist prepared under IMPETUS and reproduced below. To ensure that all actions undertaken by the involved end-users are considered ethically and legally acceptable, each entity adopting the IMPETUS tools or similar technologies must ensure its capacity to undergo proper due diligence and to ensure that all the below-listed factors are considered, understood, answered, and resolved.

This procedure aims to foster not only the developer's and deployer's dedication to legal and ethical standards concerning personal data manipulation, but additionally serves to enhance and strengthen the public perception and acceptance of such activities. Given the nature of personal data manipulation and all moral and legal hazards connected to such activities, developers and deployers must take extra steps to ensure their dedication to the relevant legal and non-legal standards and recommendation concerning the adequate measures and procedures connected to the manipulation of data and use of advanced algorithms.

List of stakeholders

In order to ensure that relevant laws and regulations are being followed, it is recommended to define the stakeholders affected by the use of smart city technologies in public security sector.

It is useful if they can be categorized into one of the following [Ethics guidelines for trustworthy AI \(EGTAI\)](#) categories:

- **developers** (research, design, development of AI system),
- **deployers** (public or private organizations that utilize AI systems for themselves or as a service to third persons),
- **end-users** (engaged with the AI system),
- **society at large** (all third parties affected by the AI system).

For **developers**, it is recommended to explore whether there are relevant stakeholders among them, and if there are, are they public or private entities. In addition, it is important to know what kind of AI system they are developing and whether they already have a legal and ethical framework in place concerning the collection and manipulation of data.

For **deployers**, it is recommended to explore whether there are relevant stakeholders among them, and if there are, are they public or private entities. Furthermore, it is important to be informed about the purpose of and the type of AI system they are utilizing as well as if they already have a legal and ethical framework in place concerning the collection and manipulation of data, do they solely rely on the AI system (full automatization), or do they insist on human operators / oversight / control.

It is recommended to explore whether there are relevant stakeholders among **end-users**, and if there are, are they public or private entities. Moreover, it is important to be aware about the purpose of and the type of the AI system they are utilizing.

Lastly, it is recommended to explore whether there are relevant stakeholders among the third parties, and if there are, are they public or private entities. Also, it is essential to know how they are affected, whether they are aware that they are affected and to what extent.

Fundamental rights' impact assessment

In order to ensure that relevant laws and regulations are being followed, it is essential to know what sort of data can be collected by the tools used (visual data, auditory data, biometric data, genetic data, documentary data, ethnical data, racial data, social data, religious data, health data, private data, and other data) and which of them are relevant for the context.

It is recommended to examine what the possible risks to fundamental data rights are while collecting this data and whether such risks are acceptable, and can a limitation or exclusion of fundamental data rights be justified by higher goals/principles.

Concerning data anonymization, it is relevant to know what are the implications of anonymized (de-identified) personal data getting re-personalized (re-identified) and does the technology in question allow for pseudonymization technics leading to untraceable data sets.

It is crucial to be aware of the potential of certain fundamental data rights precluding the collection and manipulation of personal data as well as being familiarized with boundaries to what extent private data can be collected and manipulated.

There is a difference between collecting and manipulating data for commercial purposes and security and intelligence purposes, and it is important to know to what extent.

It is relevant to understand whether human operators control private data collection and manipulation or can specific activities be fully automated and does the moment when anonymized data needs to be re-personalized constitute a valid junction for a human operator to take over the analysis from the AI system, does the AI system decide which anonymized data needs to be re-personalized or make recommendations to that effect as well as should the AI system continue with independent analysis and decision-making after the data has been re-personalized.

When informing the third-party stakeholders (citizens and private entities) about their data being collected and manipulated, it is important to define at what time and to what extent is this information to be released, are there any plausible exclusions to such a rule, should a human operator be in charge of informing the third-party stakeholders, or can this procedure be delegated to the AI system and does it make a difference if the data collected on a particular individual was relevant for the conducted investigation/surveillance.

It is valuable to investigate, if the collection and manipulation of data have led to a particular decision legally affecting individuals, whether such decisions be based on automated processing or must the human operator's consideration precede such a decision in the country of event.

Another aspect to explore in national legislation is to what extent should private stakeholders be involved in data collection and manipulation in security and intelligence operations and should the private entities be allowed to act as processors on behalf of security and intelligence agencies acting as controllers.

Lastly, important to check is whether there is any audit or external feedback mechanism in place, and is an oversight system in place.

Deployer's obligations

It is recommended to know to what extent should the AI system's operations be managed, controlled, or supervised by human operators, and what category of the AI system's governance should be employed.

It is important to decide on an established audit, supervision and/or oversight mechanism, and whether it is to be handled internally or externally. If deployer's operation is not regulated accordingly, it is necessary to ensure further regulation.

If not implemented, it is essential for the deployer to develop a data storage protocol, data access protocol, AI system's algorithm integrity and reliability protocol, AI system's algorithm decision-making protocol, human operator's decision-making protocol, data quality and integrity protocol, data processing protocol, data sets and processes traceability protocol, and other similar protocols and standard (code) of conduct specifications.

In line with the previous points, the AI system's algorithm should have clear rules on dividing surveillance-related relevant from irrelevant data. It is to be decided whether the two sets are stored jointly or separately, can a human operator access both sets or just the relevant data set, should the human operator be able to access both sets and should the irrelevant data set be stored for a specified time, or should it be deleted immediately after classification.

The AI algorithm should have clear rules on pseudonymization and the creation of traceable and untraceable data sets. It is to be decided whether the two sets are stored jointly or separately, can a human operator access both sets or just the traceable data set and should the untraceable data set be stored for a specified time, or should it be deleted immediately after classification.

It is important to identify which data are considered as traceable and which are untraceable. Under this categorization, it is relevant to decide if all data, not falling under the red-flag alert system, should automatically be pseudonymized and directed to the untraceable data set (green-flagged, cleared data) and should a human operator have the option to reverse the course and move data freely from one category to another.

It is crucial for the deployer to develop an AI system's negative impacts management system (identification, assessment, documentation, and minimization).

It is recommended to consider is to what extent does the AI system's algorithm influence the human operator's decision-making.

General ethical and legal considerations

When deciding on the use of big data in security and intelligence operations, it is important to realize to what extent does the use of big data in security and intelligence operations widen the asymmetry of information and power between the public security departments and agencies and the general public and whether the concept of data rights as fundamental human rights is then being belittled.

Furthermore, it is wise to consider to what extent do the security exigencies justify private data infringement, access to personal information, and use of private collection mechanisms (i.e., mobile phones, private CCTVs, and similar) and the security clearance negate third-party stakeholders' right to be informed over legal or illegal transgressions into their private domain.

It is important to define and consult with national legislation to what extent should security and intelligence operations concerning data collection and manipulation be regulated, supervised and oversight, should the oversight and supervision bodies be internal or external, or both and what should be the composition of such bodies be.

Moreover, it is recommended to address relevant legislation in the matter of extent to which is the redress right (right to claim for damage compensation) warranted when harm has resulted from unlawful/unfair/unethical collection and data manipulation during the security and intelligence operation, should the redress right be warranted where harm has resulted from the AI system's malicious use during the security and intelligence operation and to what extent should the redress right be warranted where harm has resulted from the AI system's malfunction during the security and intelligence operation.

Concerning the previous point, it is recommended to inform about who should be the responsible party (i.e., the agency conducting data collection and manipulation, the agency providing hardware/software, the agency in charge of the overall investigation, the ministry of interior, state) and does the existence of such a right require the presence of a mandatory liability insurance policy.

It is recommended to decide should the security or intelligence agency collecting and manipulating data have experts in ethical issues, or should each operator be trained in ethics.

It is important to explore and define how long should the anonymized and re-personalized data be kept, can it be shared with other agencies, and can it be used for purposes other than the initial investigation.

It is important to explore relevant legislation and decide should consideration be made concerning the restrictions imposed on public bodies when collecting and manipulating data be equally applied to the private sector and should each public security department and agency run separate real-time security and intelligence data collection and manipulation center, or should an emphasis be placed on joint center(s).

Privacy Enhancing Techniques for Smart Cities

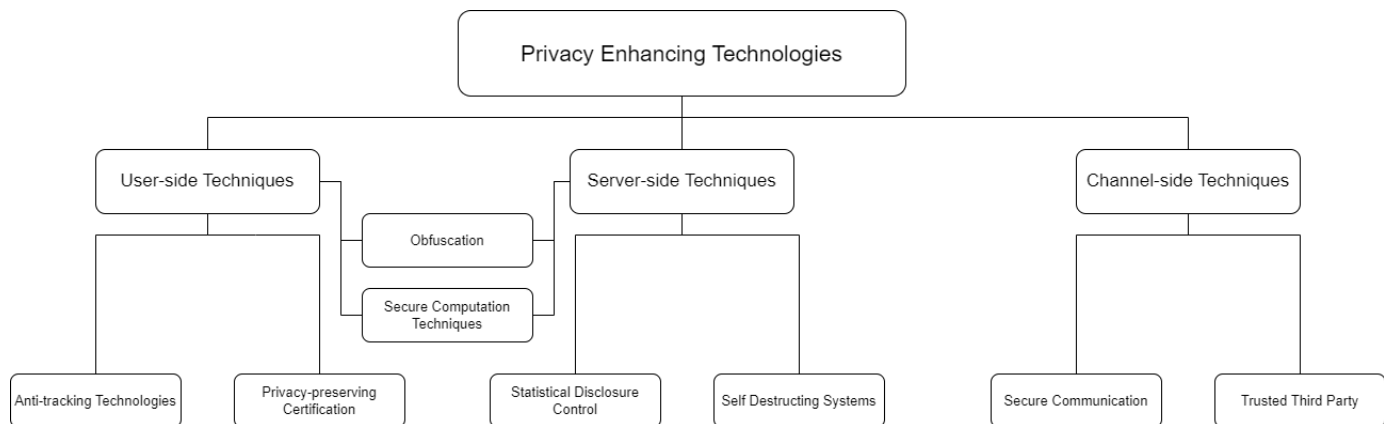
Privacy Enhancing Technologies (PETs) are technologies that embody fundamental data protection principles by minimizing personal data use, maximizing data security, and empowering individuals.

The [European Union Agency for Network and Information Security \(ENISA\)](#) defines PETs as:

'software and hardware solutions, ie systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons.'

PETs link closely to the concept of the [Privacy by Design](#) and therefore apply to the technical measures you can put in place. They are also a means of implementing data protection by design within an organization on a technical level.

The following diagram provides a visual taxonomy of PETs, divided in three main categories:



The first category, called **user-side techniques**, requires the full involvement of the end-user in order to protect his privacy. User-side methods incorporate two fundamental PETs classes specifically, anti-tracking technologies, e.g., ad-blockers and anti-finger-printings; and privacy preserving certification. It also involves two sub-categories, called data perturbation and Secure Multi-Party Computation (SMC), under the obfuscation and secure computation mechanisms, respectively.

The second category, referred to as **server-side techniques**, requires the server to be firmly engaged with the privacy protection process either by anonymizing data sets for information sharing or valorization, or by performing substantial calculation over perturbed information while collaborating with end users. Server-side methods contain two classes: the Statistical Disclosure Control (SDC) and self-destructing data systems, and two sub-categories, to be specific Private Information Retrieval (PIR) procedures and homomorphic encryption algorithms, under the obfuscation and the secure processing mechanisms, respectively. It is worth noting that the obfuscation and secure computation techniques include both user side and server-side privacy-preserving procedures, and are implemented with respect to the framework's identified objectives.

The third category named as **channel-side techniques**, specifies the nature of the channel between the client and the server - regardless of whether it is enciphered, encapsulated or encoded - or the nature of the exchanged information which can be intentionally corrupted. Channel-side procedures incorporate secure communications and Trusted Third Party such as anonymizers.

General recommendations - First, it is important to emphasize that due to the diversity of smart applications, different privacy technologies need to be combined to ensure an acceptable level of privacy. Indeed, smart cities combine so many technological components that it is not enough to simply apply privacy technologies to each component. Instead, we advise that the interactions between technologies and data have to be considered to design "joint privacy technologies." This is especially important because applications start with isolated solutions that get integrated gradually. Thus, one approach to facilitate joint privacy protection is to focus on the interfaces between different systems, on their interactions and in particular on the data flow. For example, different components in a sensor-based application may all deploy independent differential privacy mechanisms before transferring data to the processing layer. Taking this into consideration will help to define appropriate privacy enabling mechanisms for the data storage and processing.

Second, it is crucial to consider the architecture patterns that define the system's components, responsibilities, and the relationships between them. There are two main architectural design. The first group contains variations of a simple centralized architecture that does not take into account the diversity of attackers and smart city applications. The second group relies on distributed settings that are tailored to specific application areas within the smart city and may induce communication overheads.

Both joint privacy mechanisms and privacy architectures aim to integrate isolated privacy protection mechanisms into more general solutions. In smart cities, this integration is complicated not only by a large number of subsystems, but also by a large number of stakeholders. To implement joint privacy mechanisms in a coherent privacy architecture, various stakeholders should collaborate on an

operational level. However, this collaboration can entail privacy risks because it may enable stakeholders to combine data from several sources.

User-side Techniques

User-side techniques mainly aims at empowering the data owner, for instance through the implementation of user-centric data management systems.

i The user-centric data management model is introduced to automate and support users' identity management at the user side. Users are given the control over their identities, i.e., considered as a collection of attributes, and they are able to select information to disclose and to be notified when their information are collected. Users' consent is also required for any type of analysis and manipulation over their collected information. The user identity and attributes can be stored in a hardware device (e.g., smart card, portable personal device). As such, the user only needs to memorize one credential (i.e., to access to the hardware device) instead of remembering several identifiers and credentials.

Among user-side management implementations, we can mention the OpenID framework that is already used in well-known Web platforms such as [Drupal](#) and [WordPress](#). In the OpenID framework, a user can be identified by an URL (Uniform Resource Locator) or an XRI (EXTensible Resource Identifier) address. The uniqueness of URLs, resp. XRIs, makes the user uniquely identified. OpenID enables a user to choose his identity provider as well as his identity.

Various prototypes have been also proposed and considered as fundamental building blocks in privacy user-centric data management systems. Indeed, every data owner can prove to a service provider (data processor), that he holds validated properties, referred to as credentials, obtained from issuing authorities. These techniques permit to prevent service providers to -trace- users' activities based on successive communication sessions.

User-side methods attract a lot of interest and complete consideration from industries and academia, thanks to their capacity to enforce the data minimization basic component. The design of these systems strongly rely on the use of malleable cryptographic primitives that ensure several interesting properties, such as the selective disclosure feature and the unforgeability property. In fact, the selective disclosure property refers to the ability provided to the user to present to the service provider partial information extracted or derived from his certified information. For instance, to prove he is older than 18 to purchase liquors, while not revealing his birth date. The unforgeability property ensures that unless a user possesses a legitimate and certified credential, i.e., secret key, he is not able to generate a valid authentication proof, i.e., user's signature over the service provider's access policy.

Server-side Techniques

Server-side enabling technologies include three main categories, i.e., data perturbation, Secure Multiparty Computation (SMC) and database anonymization.

Data perturbation

Data Perturbation aims at intentionally making information difficult to understand or perceive for security and privacy reasons. In fact, the speed of dissemination of information, the technical progress and the global nature of the Internet make it difficult to delete data that may be too personal, embarrassing or confidential. Thus, perturbation consists mainly in publishing large amounts of information that are false, imprecise, irrelevant and/or organized in such a way that the information that one wishes to protect is hidden, i.e., embedded in a large volume of data. Data perturbation techniques are used for enhancing privacy in various querying services. In order to protect queries, one idea consists of generating dummy queries that will be sent to the central server along with the real query. The main issues of these techniques are the privacy utility trade-offs induced by the suppression technique, removing some records or details.

Secure Multi-party Computation (SMC)

Privacy preserving computation (SMC) techniques aim at protecting users' privacy and the secrecy of data contents during processing over these data. The goal of secure computation techniques is to enable distributed computing tasks among participating entities in a secure manner. That is, it considers that a group of participants wants to carry out a joint computation of a given function while keeping secret the input data of each party.

SMC has been used to solve several privacy-preserving problems such as private database queries, secret voting, privacy preserving data mining and privacy preserving intrusion detection tools and mechanisms.

Three different approaches are generally deployed to provide secure multiparty computation functionalities, namely oblivious transfer, homomorphic encryption, and secret sharing techniques. The oblivious transfer protocol generates high processing and communication overheads. The secret sharing approach gives better results in terms of computation cost, thanks to the usage of primitive operations. However, it requires the existence of secure channels between different participating entities, hence generating a high bandwidth consumption, due to the involved interactions between users. The homomorphic encryption does not require the existence of secure channels and assures a high level of privacy. However, it necessitates several processing operations to ensure homomorphism properties, thus generating high computation complexity.

Database anonymization

Database anonymization techniques are basically used to protect data within statistical databases. They permit to resolve the trade-off between data usability and users' privacy preservation, as revealed results, either the databases or a specific result over the database do not permit to reveal information related to a specific user. These techniques also include Differential Privacy mechanisms.

Anonymization techniques are relevant for various use-cases, namely applications that do not require to learn the original user's identity, but only context information. Anonymization techniques mainly refer to database privacy preservation. Even so, for cooperative applications where the database belongs to several corporations, it comes to the privacy protection of the various collaborating entities.

Main techniques for anonymizing databases w.r.t. respondent, owner and users' privacy include *k-anonymity*, *t-closeness* and *l-diversity*. Note that these techniques that are originally used over statistical databases have extended usage to dynamic data.

Differential privacy (DP) is acquiring a growing interest, primarily to guarantee security saving information mining. In a nutshell, differential privacy ensures that the removal or addition of a single database item does not (substantially) affect the outcome of any analysis (i.e., the probability distribution of released items does not significantly change). This property is enforced by adding random noise to the exact outcome.

Communication Techniques

In the context of connected cities, it is difficult to prevent pervasive surveillance over all physical connections. Indeed, it is important to protect access to public and shared resources through security mechanisms to prevent malicious entities from deducing users' patterns of browsing, profiling, service use or extracting identifiers that are transmitted through communications channels. There exist two main strategies to secure communications, namely client-service and end-to-end communications.

Client-service secure communications

To secure communications against pervasive surveillance, several service providers propose to deploy encrypted communication channels. It is important to emphasize that encrypted channels need to be implemented and configured correctly, to ensure a sufficient security level. Several technologies and protocols can be implemented, namely the well-known [Transport Layer Security 1.2 protocol \(TLS 1.2\)](#) and the [Secure Shell \(SSH\) protocols](#). These technologies provide a confidential and conceivably authenticated channel between users and service providers, but do not implement security measures between different users of the same service.

End-to-end secure communications

End-to-end encrypted services refer to encrypted communications between end-users, meaning that the encryption layer is added at one end-user and is only removed at the other end-user. Hence, transmitted data cannot be read by any third party including the service provider, e.g. [VPN based communications](#). Service providers usually need to assist users to authenticate them, in order to create an end-to-end encrypted channel. However, it is preferable that the keys used to subsequently ensure the confidentiality and integrity of data never be available to the service providers, but derived on the end-user devices.

Case Study: LEx Ethical and Privacy Considerations

The main focus of the following case study is to describe the procedures that have been followed during the testing phases of the IMPETUS tools and that could serve as guidelines for the adoption of the tools or of any similar technological instrument.

The procedures have been defined in order to have a synergical cooperation among the involved subjects (more specifically, public entities' representatives, legal and IT consultants and tools' providers) while considering and respecting all the applicable laws, guidelines and best practices.

The below attached checklist of activities to be done implies a preliminary consideration: the assessments of the regulatory compliance of the IMPETUS tools and platform have been drafted based on the use of the tools during the so-called Live Exercises ("LEx"), which took place in Oslo (Norway) and in Padova (Italy). Moreover, the compliance has been considered with a particular reference to European laws on data protection. National laws were also considered but are not reported in the checklist since they are strictly related to the context of use.

Most of the evaluations and activities described in the checklist imply the involvement of IT and legal consultants.

More specifically, the assessments of the tools and the attached checklist take in consideration:

- the security technological measures which the tool developers were able to grant during the LEx;
- the networks, technological systems and other infrastructures which were already in place in the cities of Oslo and Padova, which were directly involved in the Project;
- the fact that the LEx have been done for research purposes and they only lasted a couple of days; and
- that most of the data subjects were volunteers.

In the following checklist, it has been highlighted which evaluations have been done during the IMPETUS development and can be considered final and which activities are strictly related to the context of use and should be conducted having regard to the specific situation.

Checklist



The checklist involves the following steps:

1. Define the context of use of the tools
2. [Identify the applicable laws](#)
3. [Choose adequate security measures to prevent violations of rights](#)
4. [Grant an effective oversight](#)
5. Clearly identify the data processing activities, via a detailed description of the processing activities, the definition of data subjects and the processed personal data, the identification of the storage location and the retention period
6. Analyse the data processing activities for the tools which process a bigger amount of personal data
7. Sign a data protection agreement with each external subject that will have access to personal data as Data Processor
8. Carry out a [Data Protection Impact Assessment \(DPIA\)](#) related to the specific context of use of the tools
9. Verify if in accordance with European or national legislation a notification to data protection authorities or other authorities is required
10. Recruit the volunteers respecting the approved procedures
11. Inform the involved subjects

The detailed checklist is attached hereafter.

Checklist for the Live Exercises 2022

Summary

1. Define the context of use of the tools.....	2
2. Identify the applicable laws.....	2
3. Choose adequate security measures to prevent violations of rights.....	2
4. Grant an effective oversight.....	3
5. Clearly identify the data processing activities.....	3
6. Analyse the data processing activities for the tools which process a bigger amount of personal data (for the LEX: SMD, FD and WMS tools).....	4
7. Sign a data protection agreement with each external subject that will have access to personal data as Data Processor.....	5
8. Carry out a Data Protection Impact Assessment (DPIA) related to the specific context of use of the tools.....	6
9. Verify if in accordance with European or national legislation a notification to data protection authorities or other authorities is required.....	6
10. Recruit the volunteers respecting the approved procedures.....	6
11. Inform the involved subjects.....	6

Ethical and Privacy Assessments of IMPETUS



This section includes the analysis of the IMPETUS tools and platform from the perspective of European data protection laws and ethical guidelines. It also provides “General considerations and recommendations” which refer to issues that have not been dealt with during the testing of the tools within the IMPETUS Project, but should be considered in the event of an adoption of the tools and of the platform in real contexts, especially for public entities. From an IMPETUS perspective, the analysis provided a deep understanding and objective consideration of different regulations and standards in terms of data usage. From a general perspective, the detailed analysis aims at presenting concrete examples so that interested users can follow the same methodology when carrying out a similar assessment of other technologies they might wish to adopt.


For the **ethical analysis**, we consider relevant [EU guidelines and regulations](#). A useful tool to assess compliance could also be the [Privacy, Ethical and Social Impact Assessment \(PESIA\) questionnaire](#). The questionnaire focuses on IoT systems but can be adapted also to other technological solutions. The PESIA model has been developed by Politecnico di Torino as part of the VIRT-EU project in collaboration with scholars from the Open Rights Group, London School of Economics and the IT University of Copenhagen.

On the other hand, for the “**Data Protection Impact Assessment**” (**DPIA**), we refer to the assessment conducted following the [ENISA methodology](#) for the tools dealing with personal data and the main platform.

The section includes the following:

1. [Privacy impact assessments and ethical analysis](#)
2. [Experiences and lessons learnt - Ethical and privacy enforcement for future development](#)

Privacy Impact Assessments and Ethical Analysis

 This page includes the privacy impact assessment (PIA), following the [European Union Agency for Network and Information Security \(ENISA\) methodology](#), and provides ethical analysis of the IMPETUS tools and the platform, that are dealing with sensitive and/or personal data, based on a concrete situation.

To carry out a [DPIA](#) is a responsibility of the Data controller, in accordance with art. 35 GDPR. The Data controller shall seek the advice of the data protection officer, where designated, when carrying out a DPIA. Data processors assist the Data controller in ensuring compliance with the obligations pursuant to art. 35 GDPR, taking into account the nature of processing and the information available to the Data processor. With this in mind, the security measures applied to the IMPETUS tools were checked and mapped before the IMPETUS Live Exercises (“LEEx”). The security measures have been identified and described in accordance with the list indicated in the “[Handbook on security of personal data processing](#)”, prepared by ENISA. The privacy assessment of the tools provided hereunder is based on these lists of security measures.

Indeed, for the LEExs, the tools were connected to the Security Operation Centres (“SOCs”), networks, technological systems and other infrastructures of the different cities. The safety and the efficiency of each tool and of the data collected depended largely on the infrastructures of the cities and on their settings, and this should be considered for future implementations of the IMPETUS tools or similar technologies, as further explained [here](#).

The different analysed technologies include:

1. [UAD](#)
2. [CTDR](#)
3. [EO](#)
4. [SMD](#)
5. [FD](#)
6. [WMS](#)
7. [CTI](#)
8. [BD](#)
9. [The platform](#)

• [Urban Anomaly Detection \(UAD\) tool](#)

▼ [Context of use](#)

During the IMPETUS Live Exercises (“LEEx”) in the city of Oslo, the UAD tool collected the data on public transport that are publicly made available by the city itself. The data are timestamped instances geo-tagged with latitude and longitude (meaning the number of public means of transport and their real-time location). On the other hand, in Padova the UAD tool received data from the sensors that are located in some strategic places in the city centre. These sensors convey to the UAD tool the number of pedestrians and vehicles entering and exiting from the area, but not images.

The data and information collected could therefore change according to the specific context of use and to the instruments to which the UAD tool is connected. Indeed, the UAD tool may use different sets of data and may be connected to other tools, in order to detect anomalies related to events different than the traffic situation in a city. The UAD tool allows to elaborate data and information through big data algorithms for two main purposes: anomalies’ detection and event classification. In addition to the anomaly detector, the event classifier would be able to indicate also the type of the threat under analysis. For this task, a training phase and an event identification phase are foreseen. Combining anomalies’ detection and event classification, the tool may help identifying specific threats.

The exact functioning of the tool and the information flow have been explained [here](#).

Data Protection Impact assessment (DPIA) During the IMPETUS LEEx, the UAD tool did not process any personal data and it . For the project, the UAD tool was installed on a local server, protected by firewall and within the premises of the University of Milano. It was protected by tools available on the University’s premises (e.g., firewall) and was accessible only via VPN. It applied eEncryption of data in transit was applied. The tool collected aggregated data and numbers coming from the cameras and the SOC used by one of the cities. The images and the other data collected by the cameras were hashed within the SOC of the city. Only through the SOC it could be possible to deanonymize these data, e.g. for public security reasons. The UAD tool itself cannot deanonymize data. Moreover, the tool was not connected to the tools within the SOC which are used to deanonymize data.

Regarding the data collected by the city of Oslo, they refer to single buses. By collecting a sufficient amount of these data and comparing them with the databases of the municipality, such data may enable the identification of specific persons. This did not happen during the LEEx; therefore, a DPIA was not carried out.

Ethical issues The UAD tool integrates machine learning advanced algorithms. Human agency and oversight on the functioning of the tool and its algorithms have been considered and granted at a sufficient level.

More specifically, UAD performs the following machine learning tasks: anomaly detection (to identify data that differ from what previously observed) and classification (to classify data according to defined labels, according to what the system learned from past data). The first is an unsupervised task, while the second one is supervised. Nevertheless, an appropriate level of human control is granted. The tool provides

anomalies detection and classification as “information” to the human operator. The human operator would then interpret the data and consequently take action.

The human operator is also capable of understanding the feedback information received by the algorithm and understanding how the algorithm has produced that feedback, because the tool integrates a feature-ranking approach to provide justification of alerts generated. These mechanisms grant also a sufficient level of transparency and explainability regarding the outcomes of the algorithmic system.



General considerations and recommendations As seen with the example of the municipality of Oslo, public entities may wish to process, through the UAD tool, the location data of public transport means.

This could enable behavioural tracking of bus drivers, residents of remote areas who are usually the sole occupants of such buses in specific locations, and similar.

This is an issue that the smart city which adopts the tool has to face since there would be the need to implement security measures and protocols of use to grant a secure processing of the data of all citizens and data subjects.

Moreover, if the UAD tool will be connected to datasets containing personal data and sensitive information, the access control module should be adapted in order to perform security and privacy-aware transformations, ranging from pruning and reshaping to encrypting /decrypting or anonymizing the full resource or part of it, before giving access to data.

Having regard to an ethical use of the UAD tool, it is necessary that the users will be specifically trained in order to be able to understand the outcomes, to evaluate them and to give the right interpretation which could lead to the best decisions.

- **Cyber Threat Detection and Response (CTDR) tool**

- ✓ **Context of use**

During the IMPETUS Live Exercises (“LEx”), the CTDR tool was tested on the premises of a Security Operation Centre (“SOC”), following the usual two-step process and considering a small subnetwork.

First, the end user (usually, IT specialists and analysts and SOC operators) launches a scan of a network or sub-network with Nessus. This scan can be launched directly from the IMPETUS platform. The scan results in a file that is automatically downloaded to the end user’s PC. Nessus platform creates a graphical representation (“attack graph”) of the distribution of logs and the correlation of alerts.

After that, the file is uploaded into the CTDR tool, which runs an additional analysis of network traffic data and alerts the end user of any anomalies detected in the system. For these features, the CTDR tool is based on [Prelude OSS](#), the freeware version of Prelude SIEM3, which is a Security Information and Event Management (SIEM) tool, for the generation and reporting of cybersecurity alerts. The end user gets the alerts and a summary of the main features of the detected anomalies via Kafka bus on the IMPETUS platform, once a vulnerability has been detected. The end user can access the CTDR user interface to find additional details and remedial measures.

The tool also allows cybersecurity analysts to conduct deeper analysis of threats and countermeasures. The exact functioning of the tool and the data flow have been explained [here](#).

Data Protection Impact Assessment (DPIA) For the DPIA of the processing activities of the CTDR tool during the IMPETUS Live Exercises (“LEx”), the following information were considered:

- Processed personal data: IP addresses of network scanning devices installed on city premises. Additionally, the tool collects other information that are not personal data, such as network traffic, network scans, information about organization’s devices, and similar
- Storage location: IP addresses are saved on the premises of the Data controller (i.e., the public entity which adopts the tool), and can be processed (e.g., anonymized) before the tool and the IMPETUS platform get the new contents.
- Retention period: one month after the conclusion of each “project” (for anonymized data)
- Data processors: the use of the tool and the data processing activities do not require external data processors.

The risks related to the data processing activities, including the evaluation of the impact and the analysis of the threats, have been evaluated using the online tool provided by ENISA. The Overall impact evaluation resulted medium and the Overall threat occurrence probability resulted medium. Therefore, the risk is “medium”. The risk assessment will highly depend on the infrastructure and security measures adopted by the Data controller.

The technical and organisational security measures adopted for the LEx were considered adequate for the specific context of use. The Data controller shall consider that, according to the specific context and situation and especially to the width of the scanned network and of the collected IP addresses, further security measures may be required.

The DPIA conducted for the LEx should be implemented by information given by the Data controller, as specified hereafter. In particular, the Data controller shall:

- identify a valid legal basis for processing;
- ascertain whether the data processing activity is proportionate and necessary, or not, considering also the impact on the rights of the public entity’s employees;
- evaluate if it is required to conduct a complete DPIA in accordance [with art. 35 GDPR and to consult the Data Protection Authority as provided for by art. 36 GDPR](#);
- evaluate if a consultation of data subjects has to be done, in accordance with art. 35.9 GDPR, to seek their views on the intended processing.

Ethical issues The CTDR tool does not use machine learning, deep learning or other kinds of advanced algorithms. Data analysis is done by the logical reasoner which processes a network scan and by the algorithm developed in programming languages such as php, python and javascript.

The CTDR tool and its algorithm grant a sufficient level of human control and oversight. It does not take final decisions and only helps analysing and connecting alerts sent by different security tools. In any case, the outcomes require analysis and post-processing from IT and cybersecurity experts. The alerts received by human operators bring information about the vulnerability being exploited, the criticality (i.e., impact or collateral damages) and the possible mitigation actions. In this way, human operators are able to understand how the algorithm produced the alert. This grants a sufficient level of transparency.



General considerations and recommendations For the future use case scenarios, public entities adopting the CTDR tool should evaluate further aspects.

Firstly, the tool was created already applying the best security practices in the relevant field. This is due also to the fact that it is based on open-source software, subject to a constant “peer review”.

The choice of Kafka to share data with the IMPETUS platform is also satisfying, since **Kafka allows to encrypt the data** using a public key with the private key on the IMPETUS Platform, with any other system needing to read the data from the Kafka bus.

On the other hand, other features of the tool can be adapted to the needs of public entities and from such choices both improvements and higher risks may derive.

First of all, the file with the results of the scanning of network’s vulnerabilities will be downloaded on the premises of the public entity. Therefore, before scanning, it is fundamental to **ascertain that this file will be saved on a secure server** (either local or in cloud).

Secondly, **other software can be used instead of Nessun to scan the network**. This would require some adaptations of the CTDR tool algorithm, but the public entity will be responsible for choosing a software that grants at least the same level of efficiency and security measures of Nessus.

In the third place, it should be considered that the ability of the tool in detecting vulnerabilities depends on the knowledge graph used. This graph needs to be updated from time to time. Therefore, it is **foreseen to develop and employ a Natural Language Processing (« NLP ») model**, in order to update automatically the knowledge graph. The updating of the tool itself will be possible since it will be released as an open-source software. The use of natural language processing could lead to the rise of further issues, especially related to ethics. Ethical issues associated with [NLP](#) do not subside with the process of data generation but are recurrent at every stage, concerning learning bias and the evaluation, aggregation and deployment stages.

Lastly, **anonymization of IP addresses** collected when vulnerabilities are detected (either exploited or likely to be exploited) should be considered.

On the one hand, IP addresses detection may facilitate a deeper analysis of vulnerabilities and the prevention of future attacks. Indeed, the organisation adopting the CTDR tool could better evaluate specific countermeasures, including training of the employees.

On the other hand, the lack of anonymization of IP addresses implies the possibility to detect if the action of a specific employee contributed to the exploitation of a certain vulnerability. In this way, the tool could be considered as an **instrument to monitor workers** and to address disciplinary sanctions.

This use of the tool could lead to the breach of labour law provisions, as analysed [here](#). In general, each public entity must adapt internal procedure on how much data is stored, accessed, shared, and when are they deleted.

- **Evacuation Optimizer (EO) tool**

- ✓ **Context of use**

During the IMPETUS Live Exercises (“LEx”), the simulation of emergency situations has been performed with volunteers who were aware of the simulated nature of the emergency, even if they were required to act as naturally and spontaneously as possible. There was no real panic situation. Static pre-simulated scenarios were defined before the Live Exercises because the tool could not rely on the outputs of the counting sensors of the cities.

During the LEx, the human operator receiving the data from the tool manually searched through the guidelines uploaded on the IMPETUS platform and had to choose the right one to apply. Indeed, the EO tool may be used by the police and emergency forces to provide efficient exodus ways given different scenarios possible. It could be used both to a better management of organised events and in case of critical event. The tool can be combined with a broad communication tool and the defined guidelines may suggest using one or more other technological tools.

The exact functioning of the tool and the data flow have been explained [here](#).

Data Protection Impact Assessment (DPIA) The EO tool does not require the processing of any personal data for its functioning. For example, in cities with counter person sensors, the tool would register only the number of people crossing a specific gate at a given time and calculate the density in a specific public space. It could also elaborate historical data on the number of people in a public space in a particular period of time.

On the other hand, output data of the tool are represented by guidelines and numbers representing parameters for managing the crowd of people (time for egress, available gates, etc.), without any reference to identifiable persons.

Ethical issues The EO tool works according to the following principles: reference scenarios involving the egress of a crowd are pre-simulated in advance through a dedicated software. Results are synthesized and turned into a set of written guidelines, a video of simulated egress and a coloured risk class. The EO tool per se does not contain any algorithm. For ethical issues which may arise from its use in real-life scenarios, please refer to the general considerations and recommendations for use.



General considerations and recommendations According to the technological solutions and sensors adopted by each public entity, it could be possible to use the EO tool for evacuating public spaces during emergency situations, with the intervention of public security services.

For an efficient functioning of the tool, it is necessary that sensors can convey numbers to the tool in real-time, since any delay in the provision of information could affect the validity of the identified solution.

Moreover, it would be necessary to set the EO tool so that the identification of the suitable guideline can be automatically performed. The IMPETUS platform will then consider the exact place and the number of people counted by the sensors located in that place to show which guideline has to be followed for the evacuation process.

In such circumstances, public entities adopting the tool should adopt internal procedures in order to:

- train their employees to make them able to understand the outcomes of the EO tool;
- define parameters to identify when the EO tool has provided the best applicable guidelines and when not;
- define if the identified guidelines should always be followed and/or the margins of freedom for public security forces to disrespect the indications coming from the tool, according to their education and on-field training.

• **Social Media Detection (SMD) tool**

✓ Context of use

The SMD tool is a tool for big data visualization. Threats and insights into relevant topics may be detected by creating a “project” with some specific keywords that refer to criminal acts, illegal instruments, words of hate together with words connected with local politicians, strategic places etc.

This tool has been projected to be used by IT analysts employed in the city administration. To insert the keywords, the end-user has to access a software, which is connected to the IMPETUS tool but not to the IMPETUS Platform. The end user receives alerts on the IMPETUS Platform and on the external software once the analysis is completed. On the external dashboard, the end user may visualize the completed analysis and insights extracted.

The tool is able to collect data from social networks, social media and webpages in general. The SMD tool collects data using the API provided by the online resources or web crawling and scraping, when there is no API. The algorithm of the tool does not have access to personal data, but rather only to the messages which are provided to the machine learning models to train them. The exact functioning of the tool and the information flow have been explained [here](#).

Data Protection Impact Assessment (DPIA) For the [DPIA](#) of the processing activities of the SMD tool during the Live Exercises (“LEx”), the following information were considered:

- Processed personal data: data included in publicly available text messages on Twitter; author's id, nickname, name and location (provided by the user). Maximum 150 messages per keyword (per execution, in case of projects which are set to run periodically. A lower value may be set.
- Storage location: servers of Amazon Web Services located in Ireland during LEx. Servers of the Data controller (i.e., the public entity which adopts the tool), for real-life use cases.
- Retention period: one month after the conclusion of each “project” (for anonymized data).
- Data processors: during the LEx, Amazon. Normally, the use of the tool and the data processing activities do not necessarily require external data processors.

The risks related to the data processing activities, including the evaluation of the impact and the analysis of the threats, have been evaluated using the online tool provided by ENISA. The Overall impact evaluation resulted medium, while the Overall threat occurrence probability resulted low. Therefore, the risk is “medium”. The risk assessment will highly depend on the infrastructure and security measures adopted by the Data controller.

- ✓ The technical and organisational security measures adopted for the LEx were considered adequate for the specific context of use. The Data controller shall consider that, according to the specific context and situation, further security measures may be required. The DPIA conducted for the LEx should be implemented by information given by the Data controller, as specified [here](#).

In particular, the Data controller shall:

- identify a valid legal basis for processing;
- ascertain whether the data processing activity is proportionate and necessary, or not;
- consider that this tool could lead to a large-scale monitoring of personal data, keeping in mind that also data which are “publicly available” may still be personal data. This consideration would make the DPIA even more necessary in accordance with art. 35 GDPR and would likely lead to a consultation of the Data Protection Authority as provided for by art. 36 GDPR. Any entity adopting the tool should consider the specific settings and identify adequate security measures and legal basis;
- evaluate if a consultation of data subjects has to be done, in accordance with art. 35.9 GDPR, to seek their views on the intended processing.

Ethical issues In general, the tool and its algorithm have been developed in compliance with the rules of trustworthy AI, granting:

- Human agency and oversight
- Technical robustness and safety
- Privacy and data governance
- Diversity, non-discrimination and fairness

- Accountability.

More specifically, the machine learning models only give evaluations and classifications for different features. They do not give final decisions. It is the human operator who will have to review and analyse the results from the analysis and take all the relevant decisions and subsequent steps. The human operator is capable of understanding the feedback information received by the advanced algorithm and understanding how the advanced algorithm has produced that feedback, since there is an explainability method to explain the scores provided by the models.

Data that may lead to an identification of the user can be anonymized or pseudonymized, according to the requirements imposed by the Data controller. It is also possible to establish different levels of access to personal data, by giving only to some users and roles the possibility to unscramble pseudonymized data to return them to the original format. The key for the decryption is stored in a separate section of the system and this key is also encrypted.



General considerations and recommendations For future uses of the SMD tool or similar technologies which may be employed to monitor and analyse online interactions, critical ethical issues may arise referring to the criteria applied to create the datasets on which the algorithm for natural language processing (NLP) is trained. The algorithm of the SMD tool uses deep learning models to classify and evaluate the data acquired in real life.

It is really important that any public entity adopting the tool would conduct an audit on the used datasets before taking any decision based on the outcomes of the tool, to verify the potential presence of bias and their quality. Moreover, public entities should implement internal policies to define the aims for which the SMD tool can be used and the allowed criteria to set a new “project” with the tool. Indeed, biases may also be revealed by the choice of keywords to be looked at or of the sources to investigate.

Lastly, fairness and non-discrimination should be applied also in the interpretation of the analysis and insights extracted by the SMD tool. Therefore, it is necessary that the end users will be specifically trained in order to be able to understand the outcomes, to evaluate them and to give the right interpretation. Public entities should identify (as thoroughly as possible) the functionalities and the underlying sources of the tools and take mitigating measures in this regard to prevent unlawful conducts in the future.

Public entities should also document their choice about anonymizing or pseudonymizing the data collected and the reasons for that. The volume, nature and range of analysed personal data contribute to define the level of impact on human rights, as further explained [here](#).

If someone may have access to deanonymized data, this has to be done in compliance with all applicable laws and would probably be legitimate only if the goal is to conduct a specific investigation or to prevent serious crimes. Indeed, there is a high risk of collecting information about plenty of people and that only a small percentage of them would actually be useful.

- **Firearm Detector (FD) tool**

- ▼ **Context of use**

The FD tool performs the scanning of the footage provided by CCTV cameras to detect the presence of weapons in the video images. The scan is done by an artificial intelligence algorithm which also systematically anonymizes people's faces, blacking them out. Images are never recorded by the FD tool. When the AI detects a person brandishing or carrying a weapon, the SOC operator receives an alert through the IMPETUS platform and may see a 5-seconds video with the detected images (not obfuscated) and their geolocation on the IMPETUS dashboard. The SOC operator receives also a still image of the weapon and information about how many minutes and seconds have passed since the weapon has been detected. If the SOC operator confirms the “emergency”, the alert is shared automatically through Telegram or other communication channels with officers in the field. If the SOC operator marks the alert as not an alarm (i.e., “false positive”), the detected image of what was considered a weapon is sent back to the AI system to retrain it. In this case, the image of the “false weapon” is combined with synthetic data (not real ones).

The software which processes and analyses images is installed on an edge device, that is directly connected via LAN to the infrastructures of the public entity adopting the tool. During the IMPETUS LEx, the algorithm processed the images of some volunteers holding weapons for testing purposes. On the other hand, the training of the AI during the IMPETUS LEx took place on the premises of the developer, but can be done elsewhere if the Data controller has the required AI hardware. The AI needs to be trained for each specific context of use. During the training, raw videos are sent to the location where the AI is trained and are retained for 30 days. The exact functioning of the tool and the information flow have been explained [here](#).

Data Protection Impact Assessment (DPIA) For the DPIA of the processing activities of the FD tool during the LEx, the following information were considered:

- Processed personal data: images of volunteers;
- Storage location: images were processed on the edge device located inside the municipalities' premises and shared with the IMPETUS platform on a partner's secure servers in case of detection of an “emergency”. Data are shared via internet but in future real-life use cases, the platform itself should be installed on the premises of the Data controller;
- Retention period: until the end of the LEx. To be decided with Data controllers for future use cases;
- Data processors: subject which is responsible for the training of the AI.

The risks related to the data processing activities, including the evaluation of the impact and the analysis of the threats, have been evaluated using the online tool provided by ENISA. The Overall impact evaluation for the use of the FD tool during the LEx resulted medium and the Overall threat occurrence probability resulted medium. Therefore, the risk is “medium”. The risk assessment will highly depend on the infrastructure and security measures adopted by the Data controller, according to the description of the functioning of the tool provided in the previous paragraph.

The technical and organisational security measures adopted were considered adequate for the specific context of use of the LEx. The Data controller shall consider that, according to the specific context and situation, further security measures may be required.

Therefore, the DPIA conducted for the LEx should be implemented by information given by the Data controller, as specified here.

In particular, the Data controller shall:

- identify a valid legal basis for processing;
- ascertain whether the data processing activity is proportionate and necessary, or not;
- appropriately inform the data subjects in accordance with art. 13 GDPR;
- evaluate whether a consultation of the data protection authority in accordance with art. 36 GDPR is necessary, or not;
- evaluate if a consultation of data subjects has to be done, in accordance with art. 35.9 GDPR, to seek their views on the intended processing.

Ethical issues During the LEx, the potentially relevant ethical issues that the use of the FD tool could pose were not considered as an obstacle since only a small amount of images were made visible to SOC operators, and the tool was used for a limited period of time.



General considerations and recommendations Hereinafter we will consider the main issues that a public entity should consider when adopting the FD tool and connecting it to its CCTV cameras.

First of all, the modalities of the training of the AI should be considered. The correct functioning of the AI depends on the characteristics of the cameras, on their location, on light conditions, and so on. Therefore, to be able to process images in an efficient way, **AI has to be trained for some months with the required high-level hardware.**

Secondly, obviously many public authorities could think that **combining the technology of the FD tool with a facial recognition system** would be a desirable solution to better protect citizens. In 2021, the European Data Protection Board [called for a ban of all kinds of facial recognition systems](#). This line would probably be followed as regards private companies, but many European states still maintain [wide exemptions](#) for law enforcements to deploy such technology in cases including a search for missing children, preventing terrorist attacks or locating armed and dangerous criminals. Each public entity should therefore carefully analyse the regulatory context.

In the third place, public entities should **audit the algorithm used to obfuscate images** in order to evaluate the security level against artificial intelligence-based reconstruction attempts. Images are not recorded by the FD tool, but real-time attacks could still be possible.

Moreover, public entities and all their employees, especially SOC operators and security forces, should be specifically trained and well aware about the functioning but also about the **limitations of the AI system** of the FD tool. This should lead to the adoption of internal procedures that **define how the tool should be used and clarify that it cannot substitute human intervention or analysis**, but rather represent a help to human operators. Indeed, even with an accurate training of the AI, the capacity to detect weapons among billions of processed images could depend, for example, on the lighting, on the partial obstruction of the weapon, on the camera positioning and lens type, on the presence of rapidly moving objects, on the image resolution, and so on.

Lastly, the processing of images collected through CCTV cameras with the FD tool would represent a new processing activity, with different means and for different purposes. Therefore, **citizens should be duly informed about the intended use of the collected images.**

- **Workload Monitoring System (WMS) tool**

- ✓ **Context of use**

During the IMPETUS LEx, some volunteers who were employees of the municipality and/or of the police department wore the headband with the sensors to collect brain signals and heart rate signals. A stress situation was simulated. The sensor was connected via Bluetooth to a local device. The raw data were buffered for 5 seconds before being deleted.

Before the test, an assessment model had been created based on the normal biosignals and health related information of the individual. The features extracted from these raw data were shared via an encrypted file saved in drive with the tool developer to create the machine learning model. The machine learning models within the tool are trained on these features extracted from data that are acquired during the calibration task, which takes place offline. The assessment model had then been deployed on a secured USB drive.

The results of the analysis of biosignals collected by the sensors of the WMS tool were showed on the dashboard of the IMPETUS platform as referred to the "SOC operator".

For the use of the WMS tool or similar technologies in real-life situations, the context and ways of use could differ from the ones of the LEx for the following aspects:

- identification of the person wearing the sensor (identified with a generic name, e.g. "operator 1" or with his/her exact name). If generic names are used, there would still be the possibility for the employer to know which person is wearing which sensor in a precise moment;
- period of retention of biosignals (raw data) and/or alerts (aggregated data and outcomes);
- choice of the devices (USB drive for the model and computer with the necessary software) to be used. This would influence the security of the processing activities and the power to control and use the assessment model.

Data Protection Impact Assessment (DPIA) For the DPIA, of the processing activities of the WMS tool during the LEx, the following information were considered:

- Processed personal data: biosignals (health data) (signals through an electroencephalogram (EEG) and heart rate and flow signals through photoplethysmography (PPG)). Training data: age and information about personality and health status.
- Storage location: stored locally on a computer provided by the tool developer. Will be a device belonging to the Data controller (i.e., the public entity which adopts the tool), for real-life use cases.
- Retention period: raw training data will be anonymized immediately after the creation of the assessment model (buffered only for 5 seconds). The workload predictions are stored for 5 minutes before being deleted (the storage period can be changed according to the needs of the Data controller).

- Data processors: for the LEx, the tool developer. Normally, the use of the tool and the data processing activities do not require any data processor.

The risks related to the data processing activities, including the evaluation of the impact and the analysis of the threats, have been evaluated using the online tool provided by ENISA. The Overall impact evaluation for the use of the WMS tool during the LEx resulted high, while the Overall threat occurrence probability resulted low. Therefore, the risk is “high”. The risk assessment will highly depend on the infrastructure and security measures adopted by the Data controller.

The technical and organisational security measures adopted for the LEx were considered adequate for the specific context of use. The Data controller shall consider that, according to the specific context and situation, further security measures may be required.

The DPIA conducted for the LEx should be implemented by information given by the Data controller, as specified here

In particular, the Data controller shall:

- identify a valid legal basis for processing;
- ascertain whether the data processing activity is proportionate and necessary, or not;
- appropriately inform the data subjects in accordance with art. 13 GDPR;
- evaluate whether a consultation of the data protection authority in accordance with art. 36 GDPR is necessary, or not;
- evaluate if a consultation of data subjects has to be done, in accordance with art. 35.9 GDPR, to seek their views on the intended processing.

As for the legal basis, it should be considered that usually in the European Union consent is not recognised as a valid legal basis in the relationship between workers and employers.

Ethical issues Before the LEx, volunteers were thoroughly informed about the planned activities and the management of their personal (health) data. Moreover, information about their mental and physical health were deleted immediately after the end of the LEx.

In general, the tool and its algorithm have been developed in compliance with the rules of trustworthy AI, granting:

- Human agency and oversight
- Technical robustness and safety
- Privacy and data governance
- Accountability.

Moreover, the machine learning models are not able to be extrapolated to tasks that are outside the task learned during training or to provide accurate classifications based on data in a domain other than the training data.

Workload classifications are provided to the supervisor through the WMS dashboard. Based on the classification, the supervisor is able to assess which action is required in order to guarantee the team’s performance, therefore there is a constant involvement of human operators in the decision-making.



General considerations and recommendations For future uses of the WMS tool or similar technologies which allow workers’ monitoring through algorithms, critical issues may arise especially if such technologies imply and/or are connected to an automated decision-making instrument. But even if there is not an automated decision-making process, constant monitoring of workers could nevertheless threaten their physical safety and well-being, thus presenting ethical challenges and potential law violations. For a deeper analysis of these topics, please refer to [Experiences and Lessons Learnt](#).

It is therefore recommended to adopt internal policies to clearly inform the workers about the functioning of the tool and the intended aims for its use. It should also be clarified which parameters are used to evaluate the “workload” of workers and which are the possible consequences of the detection of a stress situation.

Having regard to an ethical use of the WMS tool, it is necessary that the users will be specifically trained in order to be able to understand the outcomes, to evaluate them and to give the right interpretation which could lead to the best decisions.

The public entity adopting the tool should also define safeguards against the potential incompetent and/or non-authorised operation of the tool, in particular by limiting functionalities for different levels of operators.

- **Cyber Threat Intelligence (CTI) tool**

- ✓ **Context of use**

The CTI tool allows end users (mainly IT specialists) detecting attacks under development, before they are deployed. Indicators of Compromise (“IOCs”), such as hashes, IPs, domains and URLs, are extracted and delivered in real-time, to help end users to block items that threaten their organization.

During the IMPETUS Live Exercises (“LEx”), the tool was tested on the premises of the SOC to detect if domains related to the involved municipalities had been compromised. In future use cases, the tool would of course allow wider analysis. The CTI tool is able to extract data from a wide range of sources including content from limited-access deep and dark web forums and markets, invite-only messaging groups, code repositories, paste sites and clear web platforms. We enrich this data with context to provide security teams with comprehensive insight into the nature and source of each threat.

The CTI tool lists threats, categorizes them, provides all the necessary details, assigns them to different users and tracks if they are “untreated”, “in treatment” or “resolved”. The alerts are divided by urgency (imminent and emerging) and by type (brand protection, compromised accounts, DDoS attack, data leak...). The CTI tool puts in front of the IT specialists a list of the threats that are being discussed and can potentially expose the network and systems of the municipality. Even though the end user can specify what type of alerts they want

to receive, he will still receive a high number of alerts and this could be distracting. To solve this issue, the CTI tool was connected to the IMPETUS platform in a way that allows showing alerts only when the CTI tool detects new threats, which are listed as “untreated” in the external proprietary platform.

The exact functioning of the tool and the data flow have been explained [here](#).

Data Protection Impact Assessment (DPIA) The CTI tool collects the following types of information: all data that can be extracted from available sources in the clear, dark and deep web, including leaked data and threatened or breached databases, plus information and data related to the public entity which uses the tool. This refers, in particular, to domain names, IPs, aliases, BINs, CVEs (Common Vulnerabilities and Exposures) of their websites, data of the executives (like the mayor), etc. This information is necessary to set the target of monitoring for the tool and to give the end users relevant alerts.

When a threat is detected, the alert and the context reported by the CTI tool may contain personal data which refer to more or less identifiable persons, according to their nature. In case of threatened or breached databases, the public entity which has adopted the tool will receive only the parts of them which relate to threats to its own organization. The analysed data were stored on Amazon Web Services servers during the IMPETUS LEX and were retained only for the duration of the LEX.

✔ For the IMPETUS LEX, the technical and organisational security measures adopted were considered adequate for the specific context of use. For future use cases, each Data controller would need to evaluate further security measures and, in particular, shall:

- identify a valid legal basis for processing. Considering the width of data processing, a substantial public interest or a law provision would be required;
- ascertain whether the data processing activity is proportionate and necessary, or not;
- evaluate whether a consultation of the data protection authority in accordance with art. 36 GDPR is necessary, or not.

Indeed, in real-life use scenarios, the provider of the CTI tool applies encryption to stored data and they are decrypted only for the sake of sharing them with the public entity.

Ethical issues The CTI tool provides alerts and insights based on collected and analysed data, but it is always possible for human operators to flag in case of false positives, by this meaning not relevant alerts. Human control and traceability are granted also by logs which detect how the algorithm works.

The explainability of the functioning of the advanced algorithm depends on the module used. Generally speaking, the algorithm applies a risk scoring calculation to different entities. In some modules, the human operator can understand how the tool calculates the risk score and which factors were taken into account. Other times, the human operator just see alerts and the threats and sources from which they originated.

⚠ **General considerations and recommendations** Considering the present regulatory context in the European Union, the CTI tool is meant to be used only by law enforcement bodies in line with the [LED Directive](#) and other related EU and national legislation.

In any case, the use of the CTI tool by public authorities could nevertheless require the definitions of boundaries and precautionary measures. In particular, the public authority adopting the tool should:

- define which sources should be monitored to detect threats, making a balance between the importance of the prevention of cyber-attacks and the collection of large amounts of data of individuals that would mainly not be involved in such attacks;
- define the storage location and the retention period since the CTI tool may potentially lead to the collection of personal data. For European public authorities, personal data should be stored within the SEE;
- adopt internal procedures to evaluate the outcomes of the tool and to establish the possible consequences for persons whose working accounts have been compromised. This topic is sometimes regulated by employment legislation in European countries, which encourages employees to warn the employer when there is a suspicion of a cyber-attack or of a credentials' theft, reassuring them with the exclusion of any reprisal.

• **Bacteria Detector (BD) tool**

✓ **Context of use**

The BD tool is an air analyser aimed at detecting microorganism's concentration in public area. The device transmit these data to a monitoring station. During the IMPETUS Live Exercises (“LEX”) the tool could be tested without originating any dangerous situation since it detects all kinds of bacteria, in whatever concentration. Non-dangerous bacteria were spread in the air during the LEX.

The tool is made up of two devices that are respectively an air-biocollector and an ATP (Adenosine TriPhosphate) analyser. The method used is ATP-metry to quantify the microorganisms in the air. In case of biological threat, the concentration in ATP will be higher due to the bacteria concentration in the air. A local interface commands the different devices, but they can be also commanded at the distance through the IMPETUS platform.

When the BD tool detects an abnormal bacterial level in a space, according to the set thresholds, it sends an alert to the IMPETUS platform, and therefore to Security Operations Centre operators, telling them what the specific value concentration is as an absolute number and in a chart to be able to monitor the evolution and how high above the threshold it has climbed. It also provides the timestamp from when the latest data was analysed and when the next one is going to be, along with the location coordinates of the affected area. Finally, the BD tool provides a list of immediate actions to be implemented as initial countermeasures, while awaiting the intervention of the specialists. The system also notifies the SOC operators when a specific sensor is undergoing maintenance. The exact functioning of the tool is explained [here](#).

Data protection and ethical issues: The BD tool collects only environmental data, in particular the concentration of bacteria in the air. It does not collect any personal data.

The BD tool is an air analyser which does not contain any advanced analysing algorithm. The lists of immediate actions to be undertaken by SOC operators is defined in advance together with the public entity adopting the tool. The aim of the BD tool in this context is just to simplify the recovery of the most suitable lists of countermeasures.



General considerations and recommendations The BD tool may present organisational and operational issues if used in real-life scenarios, considering:

- the definition of the thresholds of danger for bacteria concentration;
- the explainability of the alerts received by the SOC operators, who should be specifically trained;
- the identification of the correct initial countermeasures that the tool suggests: this feature should be declined in a different way for each public entity, since it should be aligned with safety protocols already in place; and
- the problems related to dealing with false alarms, that cannot be excluded. When receiving an alert, a trained SOC operator should be able to evaluate it, but in circumstances in which the BD tool is connected to other technological solutions, it may originate a chain of reactions (e.g., the identification and starting of evacuations procedures) which could be harder to control and to stop.

Regarding cybersecurity, ports of the BD tool are closed and data are sent to the IMPETUS platform with a secure Kafka protocol.

- **The platform**

- ✓ **Context of use**

The main feature of the platform is a dashboard which allows the end user interacting with the tools of interest. There is a full integration with the platform of some tools, some others are only partially integrated. In case of full integration, the tool can be used only through the IMPETUS platform since it does not have any proprietary interface. If the tool collects data, these are shared with the IMPETUS platform and saved on its servers.

In case of partial integration with the tools, the IMPETUS platform dashboard shows alerts coming from the tools. For more specificities on the sources and reasons for the alerts, the end user accesses the tools through the widgets provided in the dashboard. Besides the login interface, four main areas can be identified in the IMPETUS platform user interface: the side bar, the home page, the chat and the tool alerts /dashboards. The exact functioning of the platform and the data flow are described [here](#).

Data Protection Impact Assessment (DPIA) For the [DPIA](#) of the processing activities of the platform during the IMPETUS Live Exercises (“LEEx”), the following information were considered:

- Storage location: stored locally on the servers of the platform provider. Servers of the Data controller for real-life future uses;
- Retention period: for the duration of the LEEx.

During the IMPETUS LEEx, the platform could collect personal data only from the Firearm Detector and the Workload Monitoring System tool. Moreover, the platform may occasionally process personal data if they are contained in the messages sent through the chat. The chat is meant to convey technical feedbacks or requests of support therefore it should not be used to share personal data. The use of the platform and the related data processing activities performed by any public entity do not require any data processor.

Having regard to the [FD tool](#), it shares images from CCTV cameras. The AI in the FD tool scans the footage provided by cameras to detect the presence of weapons in the video images. To protect privacy, the AI systematically anonymizes people’s faces, blacking them out. These images are never recorded. When the FD tool detects an alert, it asks the SOC operator to evaluate and confirm it. In this context, the tool and the platform process the following data:

- a) jpeg snapshots with a visual bounding box of the anomaly (i.e., gun or assault rifle);
- b) video sequence of the red alert with a visual bounding box of the anomaly;
- c) a raw video sequence of the alert (clean of any bounding box). here the person holding the weapon will be visible;
- d) GPS coordinates of the red alert (and therefore, of the person holding the weapon).

If the dispatcher of the SOC validates the alert as “Emergency”, the alert is shared using the SOC (Security Operation Control) room protocols.

As regards the [WMS tool](#), the platform allows the end users (usually, SOC supervisors) to receive alerts when the workload of an employee wearing a specific sensor is considered excessive. The alert is associated to the employee. The data controller must evaluate whether to show the exact name of the employee or rather to show anonymous indications such as “sensor 01 – Excessive workload”. The latter allows to reduce the processing of personal data through the platform.

The risks related to the data processing activities during the LEEx, including the evaluation of the impact and the analysis of the threats, have been evaluated using the online tool provided by ENISA. The Overall impact evaluation for the use of the platform during the LEEx resulted medium and the Overall threat occurrence probability resulted medium. Therefore, the risk was “medium”.

The technical and organisational security measures adopted during the LEEx were considered adequate for the specific context of use. In particular, it was considered that the platform implements role-based access. The access to the different tools is possible only for specific types of end users (SOC operators, SOC supervisors, IT specialists, IT supervisors, intelligence analysts and technical administrators).

The DPIA conducted for the LEx should be implemented by information given by the Data controller, as specified [here](#), since the risk assessment highly depends on the security of the infrastructure on which the platform is installed.

In particular, the Data controller shall:

- identify a valid legal basis for processing;
- ascertain whether the data processing activity is proportionate and necessary, or not;
- appropriately inform the data subjects in accordance with art. 13 GDPR;
- evaluate whether a consultation of the data protection authority in accordance with art. 36 GDPR is necessary, or not;
- evaluate if a consultation of data subjects has to be done, in accordance with art. 35.9 GDPR, to seek their views on the intended processing.

Ethical issues The IMPETUS platform itself does not implement any algorithm. It only shows the results and the alerts produced by the algorithms of the various tools.

The IMPETUS platform allows end users an easier access to the tools of interest, which can be all or only a selection of them. The ethical issues to be considered are represented by the issues raised by the single tools. Sometimes the concerns underlined with respect to one tool may be enhanced by the connection of the use of that tool with other.



General considerations and recommendations According to the choice of the tools that each public entity will make, it should consider the general recommendations related to those specific tools, presented in the paragraphs here above.

Experiences and Lessons Learnt - Ethical and Privacy Enforcement for Future Development



Through the development of the different tools and the platform, IMPETUS carefully considers raised issues through the various ethical, legal and data privacy assessments.

This section:

1. provides [detailed steps to carry out an effective DPIA](#).
2. includes experiences with IMPETUS, while identifying different measures to deal with [workers' monitoring concerns that are raised during the PIA](#).
3. provides [guidances and recommendations for the analysis of Big Data](#) gathered in the context of a smart city.
4. presents considerations to follow when [dealing with social media analysis tools](#).

These recommendations aim to serve as possible measures that may be enforced by the organisations implementing or wanting to implement IMPETUS tools or similar technologies.

How to conduct an effective DPIA?

For the DPIA, the Data controller (*i.e.* the public entity adopting the tool) is asked to exactly define the use case scenario and to describe the activities which imply the processing of personal data. It should be clarified from the beginning: which categories of personal data are processed, for how long and where they will be stored, who are the data subjects.

To carry out a DPIA is a responsibility of the Data controller which shall seek the advice of the data protection officer, where designated, and the Data Processors. With this in mind, the security measures applied to the IMPETUS tools were checked and mapped before the IMPETUS Live Exercises ("LEX"). The security measures have been identified and described in accordance with the list indicated in the ["Handbook on security of personal data processing"](#), prepared by ENISA. The privacy assessment should therefore consider the following steps:



- The Data Protection Officer (DPO) of the Data controller starts the DPIA by carrying out the "impact evaluation", which represents the evaluation of the impact on the fundamental rights and freedoms of the individuals, resulting from the possible loss of security of the personal data.
- The next step is represented by the "threat analysis", which is made together by technicians and DPOs. A threat is any circumstance or event, which has the potential to adversely affect the security of personal data. The goal for the Data controller is to understand the threats related to the overall environment of the personal data processing (external or internal) and assess their likelihood (threat occurrence probability).
- After evaluating the impact of the personal data processing operation and the relevant threat occurrence probability, the evaluation of risk is possible. In accordance with the verified level of risk, the DPO will be able to identify the technological and organisational security measures which are necessary and sufficient to reduce the risk to an acceptable level.
- Organisational security measures should be adopted by the Data controller, while the technological security measures combine those already provided by the tool developer with the ones existing on the Data controller's premises and infrastructure.
- If the DPO establishes that the implemented security measures are not adequate, the tool provider should consider adopting additional measures, where possible, in order to mitigate the risk to an acceptable level.
- All the different phases of the DPIA shall be reported in a dedicated document.
- Together with the analysis of the impact assessment, it is recommended to consider other kinds of law provisions which are strictly related to privacy or ethics topics. Nevertheless, it is important to remind that not everything that is not forbidden by laws, is allowed. There are already on the market many solutions for physical and cyber security which sometimes have already been adopted by various (especially private) entities and organizations and which are subject only to little regulation or oversight.

As [noticed](#), the use of advanced technologies, for example in video surveillance, is often dictated by a client's budget, not by considerations of their impacts on human rights, or similar. Similarly, limits on the use of intrusive technologies are often dictated by market forces rather than regulation. Every day new technology capabilities and offerings are being added to the marketplace with little consideration of how they will impact (human) security.

How to deal with workers' monitoring?

There are many tools, like the Workload Monitoring System ("WMS") tool, whose aim is to monitor the workload and the mental and physical status of workers in order to provide timely feedback and assure the operators can perform their tasks without being overloaded or overstressed. Such tools are usually used to prevent circumstances in which their work might be impeded, or there is unwanted fatigue and stress, reducing the effectiveness of the operators.

These functions of the tools are evaluated as important and useful in a working environment. Indeed, in a [recent paper by OECD](#), the Organisation underlined various positive aspects of this kind of instruments which make use of AI algorithms and which are defined as "**emotion AI systems**". They can be developed and implemented to detect non-verbal cues, including body language, facial expressions and tone of voice, in order **to detect workers who are overworked and those whose mental well-being is at risk**.

On the other hand, if these systems are not implemented well, they can **threaten the physical safety and the well-being of workers, thus presenting ethical challenges** and potential law violations. If employees of a security operations centre ("SOC") are asked to wear the devices and the sensors, like the ones which are part of the WMS tool, their physical status, revealing their emotions, would be constantly monitored by the supervisor in charge. In the worst-case scenario, workers could be subject to disciplinary sanctions and they could be fired or demoted as a consequence. Moreover, the use of AI systems for systematic management leads to the risk of a reduction of space for workers' autonomy and agency to the point where workers are deprived of dignity in their work. The OECD in its recent Paper reported, as an example of excessive monitoring, the use in some call centres of devices which give feedback to employees on the strength of their emotions to alert them of the need to calm down.

More specifically, the WMS tool is not an instrument for automated decision-making since every decision based on the outputs of the tool can be taken only by humans. This is compliant with the GDPR which provides individuals with the right not to be subject to automated decisions that have significant effects. In any case, there is still the risk that workers could be evaluated on the base of their physical and emotional reactions, which could not reflect their actions. Therefore, privacy and ethical considerations should be a deciding factor in the degree of automation that is chosen for algorithmic management in the workplace.

Data protection

AI can be used in different situations in the workplace. It can be used in the hiring and recruitment process, in assisting or augmenting workers, in assisting management, and finally in providing human resource services, such as training or healthcare plans. At this regard, data protection laws complement - but do not prevail on - employment legislation. Therefore, these pieces of legislation need to be considered together.

The **nature of the personal data collected** by the WMS tool, for example, may raise further concerns about possible privacy breaches and violations of human integrity or dignity. This could happen especially with wearable devices which can capture sensitive physiological data on workers' health conditions, habits, and possibly the nature of their social interaction with other people, as reported by the OECD Paper. For example, analysis of heart-rate variability provides insights into the emotional and physical endurance of employees; while this information can be collected and used to improve employees' health and safety, it can also be used by employers, even involuntarily, to inform consequential judgments.

Possible solutions and further considerations:

In considering the question of surveillance of workers, it must always be borne in mind that while workers have a right to a certain degree of privacy in the workplace, this right must be balanced against the right of the employer to control the functioning of his business and defend himself against workers' action likely to harm employers' legitimate interests, for example the employer's liability for the action of their workers. The need for a "balancing test" has been clarified already in 2002 by the WP Art. 29 in its "Working document on the surveillance of electronic communications in the workplace". The functioning of the "business" becomes more relevant in the context of smart cities which use the tool for SOC operators who are responsible for the safety and security of the city and of all its inhabitants.

Therefore, before being implemented in the workplace and even before requiring the due authorizations, any monitoring measure must pass an assessment. The questions indicated by the WP Art. 29 to summarise the nature of this assessment are the following:

1. a) is the monitoring activity transparent to the workers?
2. b) is it necessary? Could not the employer obtain the same result with traditional methods of supervision?
3. c) is the processing of personal data proposed fair to the workers?
4. d) is it proportionate to the concerns that it targets?

Moreover, it should be also clear that any personal data held or used in the course of workers' monitoring must be adequate, relevant and not excessive for the purpose for which the monitoring is justified. Any monitoring must be carried out in the least intrusive way possible. It must be targeted on the area of risk, taking into account data protection rules (at this regard, see also Articles 7 and 8 of the EU Charter of Fundamental Rights and WP Art. 29, "Opinion 8/2001 on the processing of personal data in the employment context").

At this regard, it is important to underline that the features extracted from biosignals are buffered for one minute before being deleted and the workload predictions are stored for 5 minutes before deletion. Therefore, it is not possible to have a "history" of the biosignals collected from a specific employee.

Informing individuals of their interactions with AI systems in the workplace is another fundamental element of ensuring transparency in AI system use.

An additional element of accountability lies in auditability. A number of firms are beginning to conduct audits to ensure that algorithms and AI systems are trustworthy. In the workplace, these audits have especially been concerned with discrimination or in anticipation of regulation. There are however a number of pre-requisites that AI audits need to satisfy in order to ensure accountability. Furthermore, not all AI systems are effectively auditable, especially if companies do not provide enough access and independence to auditors.

Additional cybersecurity measures will also be important in order to grant a safe adoption of the HCI tool by smart cities, in consideration of the nature of data collected.

Ethics should also be taken into consideration. When the AI is used in assisting management, as it would be the case with the WMS tool, the smart cities will need to adopt (or ask to adopt) technical and organisational measures to avoid, in particular:

- inability to rectify performance decisions;
- lack of explainability about management decisions;
- excessive monitoring.

In conclusion, a smart city which wants to adopt the WMS tool must ensure to be compliant with:

- data protection regulations at the national and international level;
- soft law and future legislation on the lawful and trustworthy use of AI, to grant the respect of principles such as human oversight and transparency, especially applied to the workplace;
- labour law, which limits the monitoring of workers and requires their prior information and prior agreements with workers' representatives.

How to deal with Big Data analytics?

Among the IMPETUS tools, the UAD tool is specifically intended for the analysis of big data. During the IMPETUS Live Exercises, it processed and analysed traffic data, but the tool could be adapted also to different context of analysis and connected to different datasets.

The exact use of the UAD tool during the IMPETUS Live Exercises and its assessment has been described [here](#), but it is worth it to consider other issues that may arise in different contexts of use, considering previous experiences with other technological tools. Big data analytics describes the science in which raw data is analyzed in order to find trends and answer questions. It involves collecting, inspecting, cleaning, summarizing and interpreting collections of related information in order to find patterns. Communications, data and datasets could be either public or proprietary, provided by clients and organizations. The latter is usually the case of datasets coming from police departments, military defense departments, etc.

An interesting case study at this regard is the software Palantir, used by many police departments in the United States and which has been the subject matter of various analysis and criticism, especially since its use spread after 9-11.



Regardless of the specific use of the Palantir made by the United States' police and the possible biases which could originate from that, we would like here to focus on the **issues that could arise from the use of the UAD tool or similar technologies, with algorithms for big data analytics**, in different ways and contexts. It should be considered whether and to what extent the collection and analysis of data is related to actual investigations on real crimes, or if it is done to prevent crimes. In the second circumstance, it appears harder to justify the gathering and merging of big quantities of data.



General considerations for future uses

- **License plate reader** The UAD tool can be connected to sensors which monitor the vehicles passing by in a specific place. Such sensors convey images to the SOC, but during the IMPETUS live Exercises images were immediately anonymized within the SOC before being conveyed to the tool. Indeed, when there are public security reasons to do that, images can be deanonymized at the SOC level and the tool be used for the analysis of different types of data (images). Images could for example refer to license plates, without conveying more sensitive personal data. The relevance and the impact of a license plate reader on the rights of citizens **highly depend on the place in which it is located**. Indeed, [some recent reports](#) focused on the use of automated license plate readers that in the United States were sometimes mounted outside emergency rooms to build out networks of victims' associates. Police had the assumption that family or friends would often drop off an injured person and then speed away. With the automated license plate reader, police can use plate numbers to determine who else was connected to the victim, even if there was no other evidence linking them to a crime.
- **Images collection** In the case of license plate readers, it was reported that they **could actually collect also images of objects and persons around the car**. These images, collected by police departments, sometimes showed the faces of people who were stopped with a person of interest. [In this way, those people too became data](#). It is evident that the less the big data analysed are personal data, the minor is the potential impact on human rights.
- **Involvement of external persons** For the use of the UAD tool or similar complex technologies, it is important that the users will be specifically trained **in order to be able to understand the outcomes**, to evaluate them and to give the right interpretation, which could lead to the best decisions. Intended users within public entities should develop the necessary competences to manage the tool and its outcomes, in order to prevent the necessity to involve external counsellors (e.g., informatic engineers) to help them evaluating the results, since this would **imply the sharing of sensitive information with non-authorised persons**. For example, this did not happen [in the case of Palantir](#). Indeed, to make sense of Palantir Gotham's data, police often need input from engineers. Only these engineers are able to analyse results and use the necessary filters to reduce the possible results to a useful number that could enable

the identification of a specific person with specific characteristics. The problem is that in this way it is up to the engineers to make assumptions in order to set filters to elaborate the results. Such assumptions (e.g., that the car was likely made between 2002 and 2005, that the man was heavy-set etc.) could easily throw off the result.

- **Merging of data** Last but not least, even if the UAD tool or similar technologies are not specifically used to process and analyse personal data or other sensitive information, their use could nevertheless **become critical when merging different types of data and datasets**. Going back to the example of the Palantir Gotham, it allows merging data from crime and arrest reports, automated license plate readers, rap sheets, and other sources. In this way, also apparently “harmless” information could contribute to decisions which have a relevant impact on citizens.

What considerations should be fulfilled by social media analysis tools?

When considering the impact of technologies used by public authorities to provide security services, **a balance has to be found between the impact on human rights and the harm that could derive from the commission of crimes**, slaughters and, in general, acts of physical violence. Tools like the Social Media Detection (“SMD”) make this balance harder. Indeed, it does not contribute to prevent actual violent crimes, such as an immediate bacteriological attack or a gunfire. Instead of this, the SMD tool allows the collection and analysis of big amount of data to identify networks of people and the interconnection of messages and actions related to the same topic, location or person. The exact use of the SMD tool during the IMPETUS Live Exercises and its assessment have been described [here](#), but it is worth it to consider other issues that may arise in different contexts of use, considering previous experiences with similar technological tools.

Generally speaking, **the SMD tool offers an Open Source Intelligence (OSINT) platform**, which allows the collection of publicly-available material. The software is able to query multiple online sources of data simultaneously and aggregate them into a single searchable source which can contain a lot of records. In particular, social media services grant the access to data collected by third vendors on a commercial basis.

It is important to consider and to understand that the volume, nature and range of personal data in automated OSINT tools **may lead to a more serious violation of fundamental rights than consulting data from publicly accessible online information sources**, such as publicly accessible social media data or data retrieved using a generic search engine, as it has recently been underlined in [an official Report](#).

- ❗ **Use of publicly available information: applicable laws and authorities’ binding decisions** As stated above, information and personal data which are collected either by commercial vendors or by public authorities (e.g., for open data projects) usually can be used only for specific purposes that are clearly communicated to data subjects. The use of these data and information for further purposes, including for public security, is legitimate only if allowed by provisions of law. **Laws may regulate both the sources that can be used and the means to process the data**. For example, in various European States laws have been adopted to regulate the use of open-source investigation by intelligence and security services and/or by other governmental bodies. Such provisions may have been inserted in criminal procedure codes, in new codes or acts and are usually complemented by decisions and ethical standards issued by Data protection authorities.

Moreover, there are already some Court decisions which clarify the correct interpretation and the scope of application of OSINT regulations. Indeed, the most famous and relevant study case on this topic can be found outside Europe, in the United States, where military services bypassed judicial supervision by purchasing location information from third party brokers. Various newspapers reported that US military agencies and the Department of Homeland Security were buying mobile phone location data from third-party brokers to trace present and past movements of users without judicial supervision. This practice continued even though [a 2018 Supreme Court](#) ruling found that the US Constitution’s protections against “unreasonable searches and seizures” required governmental officials to get a judicial warrant in order to obtain the same information directly from phone companies. Because this information is freely available on the market, US military officials maintain that they should also be able to buy this information, even though it is used for law enforcement purposes.

- ❗ **Balance between the interests at stake** The huge amounts of information shared on social media platforms may be analyzed by sophisticated algorithms to create personal profiles of users, including consumer preferences, political opinions, sexual orientation /preferences, and so on. This personal information can also be obtained by governments and used to identify and target individuals, particularly by governments with autocratic tendencies. [In various reports](#), many stakeholders from the civil society expressed an **uneasiness with the large amount of data that was being collected** everyday about the most personal aspects of their lives. Several recounted instances of when this information was used to surveil and identify targets and persons of interest and resulted in serious **human rights impacts including restrictions on travel, psycho-socio-economic costs and even arrest, bodily harm and death**.

There is the fear that softwares like the SMD tool (if used in a certain way), which have powerful data analytics and sentiment analysis capabilities may contribute to a “Big Brother” **mass surveillance** ecosystem, which can have a chilling effect on freedom of thought, opinion and expression, discouraging free discourse and expression online and offline, even in circumstances where expression is not concretely blocked. This may not only impact freedom of expression and freedom of opinion, but also rights such as those related to health and well-being.

Warranties against this misuse of such technological tools should be provided by the legislator, but also by the practices developed within governmental bodies, which should always keep in mind and not underestimate the necessary balance between all relevant human rights.

Further Reading and Standards

This page includes further references and standards that are related to privacy issues and ethical considerations in urban spaces.

- **EU Rolling plan for ICT standardisation**

The latest EU Rolling Plan provides an overview of the needs for ICT standardisation activities to be undertaken in support of EU policy activities (<https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2022>)

- **Ethics References**

1. The ICT for Peace foundations conducted a [review](#) of main commercial actors that are using information and communications technologies (ICTs) in the provision of private security services.
2. The [UK roadmap and vision on AI assurance and transparency](#)
3. The [IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems](#) ("The IEEE Global Initiative") is that Ethically Aligned Design will provide pragmatic and directional insights and recommendations, serving as a key reference for the work of technologists, educators and policymakers in the coming years.

- **Data privacy standards, guidelines and reports**

1. ISO/IEC 27001, [ISO/IEC 27701](#) covers management of risks related to Personally Identifiable Information (PII) and aids compliance with GDPR regulations.
2. [ENISA Data Privacy and Data Protection by Design report](#) contributes to bridging the gap between the legal framework and the available technological implementation measures by providing an inventory of existing approaches, privacy design strategies, and technical building blocks of various degrees of maturity from research and development.
3. [ENISA Data Protection Engineering report](#) presents existing (security) technologies and techniques and discusses possible strengths and applicability in relation to meeting data protection principles as set out in Article 5 GDPR.
4. The [Guidelines published by The European Data Protection Board](#) give general guidance on the obligation of Data Protection by Design and by Default set forth in Article 25 in the GDPR.

- **Suggested further reading lists**

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

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

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

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

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

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

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.

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

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

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

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

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

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

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

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.

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)

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

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

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

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.

Harmonized Evaluation, Certification and Testing of Security products (HECTOS). Project funded by the European Community's Seventh Framework Programme FP7/2007-2013 under Grant Agreement No 606861, 2015

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.

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.

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

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

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

OECD (2019). *Recommendation of the Council on Artificial Intelligence*. OECD/LEGAL/0449

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

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)

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)

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

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

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

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

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.

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

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

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

Practitioners Guide on Cybersecurity

Introduction and Readers Guide: Cybersecurity

What is cybersecurity about?

Cybersecurity: Quick
Intro

Principles of
Cybersecurity

Social
Considerations

How do we manage cybersecurity?

Managing Cyber
security: Quick Intro

Cybersecurity for
Smart Cities

Cybersecurity Crisis
Management

Context for Future
Adaptation

Where can we find more information?


Regulations Related
to Cybersecurity

Cybersecurity
Library

How can we assess cybersecurity in Smart Cities?

Cybersecurity Checklist for Smart Cities

Introduction and Readers Guide: Cybersecurity

 The set of materials related to Cybersecurity provides the requirements for prevention and counteraction of risks in the cyber-physical space of Smart Cities' technological architecture. It describes the IMPETUS approach as an example of measures applied to consolidate and manage cybersecurity in Smart City contexts, in order to ensure a safe and reliable environment for the citizens and for the public administration.

For an open reading experience, the root page of the [Practitioners Guide on CYBERSECURITY](#) can be accessed and explored as desired.

The reading paths below offer suggestions for specific audiences, to ease their orientation within the set of materials related to Cybersecurity and in correspondence with other subjects approached by the Practitioners Guides. The refined reading suggestions are built mainly for:

SOC Operators	Users of security solutions (for example, IMPETUS Users)
SOC Supervisors	
IT personnel	
Intelligence Analysts	
Other users	
Government Staff	General users
Decision Makers	
Policy Makers	
Regulators	
Civil Servants	
Regular Citizens	

The "IMPETUS users" category addresses the personnel that work in the IMPETUS context.

The "General users" category addresses any other readers concerned of cybersecurity aspects in relation to Smart City contexts.

Reading suggestions for SOC Operators

#reading_order	Section/ Chapter
1	Essential Ideas for IMPETUS Users
	Cybersecurity for Smart Cities
2	3. High level and horizontal synchronization
3	4. Specific vulnerabilities and threats
	Cybersecurity Crisis Management
4	1. Incident management
5	2. Cooperation and reporting

6	3. High availability
7	4. Operational landmarks
	Context for Future Adaptation
8	1. Perspectives for technology evolution
9	2. Glimpse on the evolution of cybersecurity risks
10 (optional)	Essential Ideas for General Users
(optional)	Principles of Cybersecurity
11 (optional)	3. Nuances of Cybersecurity
12 (optional)	4. Cybersecurity approaches
13 (optional)	5. The human link
14 (optional)	6. Action pillars
15	Regulations Related to Cybersecurity
16	Cybersecurity Library
17	Cybersecurity Checklist for Smart Cities

Reading suggestions for SOC Supervisors

#reading_order	Section/ Chapter
1	Essential Ideas for IMPETUS Users
	Cybersecurity for Smart Cities
2	1. Levels of integration
3	2. Protection mechanisms
4	3. High level and horizontal synchronization
5	4. Specific vulnerabilities and threats
6	5. Essential lines of action
	Cybersecurity Crisis Management
7	1. Incident management
8	2. Cooperation and reporting
9	3. High availability
10	4. Operational landmarks
	Context for Future Adaptation
11	1. Perspectives for technology evolution
12	2. Glimpse on the evolution of cybersecurity risks
13	3. Needs for adaptation
14 (optional)	Essential Ideas for General Users
(optional)	Principles of Cybersecurity
15 (optional)	3. Nuances of Cybersecurity
16 (optional)	4. Cybersecurity approaches
17 (optional)	5. The human link

18 (<i>optional</i>)	6. Action pillars
19	Regulations Related to Cybersecurity
20	Cybersecurity Library
21	Cybersecurity Checklist for Smart Cities

Reading suggestions for IT personnel

#reading_order	Section/ Chapter
1	Essential Ideas for IMPETUS Users
	Cybersecurity for Smart Cities
2	1. Levels of integration
3	2. Protection mechanisms
4	3. High level and horizontal synchronization
5	4. Specific vulnerabilities and threats
6	5. Essential lines of action
	Cybersecurity Crisis Management
7	1. Incident management
8	2. Cooperation and reporting
9	3. High availability
10	4. Operational landmarks
	Context for Future Adaptation
11	1. Perspectives for technology evolution
12	2. Glimpse on the evolution of cybersecurity risks
13 (<i>optional</i>)	Essential Ideas for General Users
(<i>optional</i>)	Principles of Cybersecurity
14 (<i>optional</i>)	3. Nuances of Cybersecurity
15 (<i>optional</i>)	4. Cybersecurity approaches
16 (<i>optional</i>)	5. The human link
17 (<i>optional</i>)	6. Action pillars
18	Regulations Related to Cybersecurity
19	Cybersecurity Library

Reading suggestions for Intelligence Analysts

#reading_order	Section/ Chapter
1	Essential Ideas for IMPETUS Users
	Cybersecurity for Smart Cities
2	1. Levels of integration
3	2. Protection mechanisms
4	3. High level and horizontal synchronization
5	4. Specific vulnerabilities and threats

6	5. Essential lines of action
	Cybersecurity Crisis Management
7	1. Incident management
8	2. Cooperation and reporting
9	4. Operational landmarks
	Context for Future Adaptation
10	1. Perspectives for technology evolution
11	2. Glimpse on the evolution of cybersecurity risks
12	3. Needs for adaptation
13 (optional)	Essential Ideas for General Users
(optional)	Principles of Cybersecurity
14 (optional)	1. Technology in our lives
15 (optional)	2. Cybersecurity - the security of technology
16 (optional)	3. Nuances of Cybersecurity
17 (optional)	4. Cybersecurity approaches
18 (optional)	5. The human link
19 (optional)	6. Action pillars
20 (optional)	Social Considerations
21	Regulations Related to Cybersecurity
22	Cybersecurity Library
23	Cybersecurity Checklist for Smart Cities

Reading suggestions for other IMPETUS users

#reading_order	Section/ Chapter
1	Essential Ideas for IMPETUS Users
	Cybersecurity for Smart Cities
2	1. Levels of integration
3	2. Protection mechanisms
4	3. High level and horizontal synchronization
5	4. Specific vulnerabilities and threats
6	5. Essential lines of action
	Cybersecurity Crisis Management
7	1. Incident management
8	2. Cooperation and reporting
9	3. High availability
10	4. Operational landmarks
	Context for Future Adaptation
11	1. Perspectives for technology evolution

12	2. Glimpse on the evolution of cybersecurity risks
13	3. Needs for adaptation
14 (optional)	Essential Ideas for General Users
(optional)	Principles of Cybersecurity
15 (optional)	1. Technology in our lives
16 (optional)	2. Cybersecurity - the security of technology
17 (optional)	3. Nuances of Cybersecurity
18 (optional)	4. Cybersecurity approaches
19 (optional)	5. The human link
20 (optional)	6. Action pillars
21 (optional)	Social Considerations
22	Regulations Related to Cybersecurity
23	Cybersecurity Library
24	Cybersecurity Checklist for Smart Cities

Reading suggestions for Government Staff

#reading_order	Section/ Chapter
1	Essential Ideas for General Users
	Principles of Cybersecurity
2	1. Technology in our lives
3	2. Cybersecurity - the security of technology
4	3. Nuances of Cybersecurity
5	4. Cybersecurity approaches
6	5. The human link
7	6. Action pillars
8	Social Considerations
9	Essential Ideas for IMPETUS Users
	Cybersecurity for Smart Cities
10	1. Levels of integration
11	2. Protection mechanisms
12	3. High level and horizontal synchronization
13	4. Specific vulnerabilities and threats
14	5. Essential lines of action
(optional)	Cybersecurity Crisis Management
15 (optional)	2. Cooperation and reporting
16 (optional)	4. Operational landmarks
	Context for Future Adaptation

17	1. Perspectives for technology evolution
18	2. Glimpse on the evolution of cybersecurity risks
19	3. Needs for adaptation
20	Regulations Related to Cybersecurity
21	Cybersecurity Library

Reading suggestions for Decision Makers

#reading_order	Section/ Chapter
1	Essential Ideas for General Users
	Principles of Cybersecurity
2	1. Technology in our lives
3	2. Cybersecurity - the security of technology
4	3. Nuances of Cybersecurity
5	4. Cybersecurity approaches
6	5. The human link
7	6. Action pillars
8	Social Considerations
9	Essential Ideas for IMPETUS Users
	Cybersecurity for Smart Cities
10	1. Levels of integration
11	2. Protection mechanisms
12	3. High level and horizontal synchronization
13	4. Specific vulnerabilities and threats
14	5. Essential lines of action
(optional)	Cybersecurity Crisis Management
15 (optional)	2. Cooperation and reporting
16 (optional)	3. High availability
17 (optional)	4. Operational landmarks
	Context for Future Adaptation
18	1. Perspectives for technology evolution
19	2. Glimpse on the evolution of cybersecurity risks
20	3. Needs for adaptation
21	Regulations Related to Cybersecurity
22	Cybersecurity Library
23	Cybersecurity Checklist for Smart Cities

Reading suggestions for Policy Makers

#reading_order	Section/ Chapter
1	Essential Ideas for General Users

	Principles of Cybersecurity
2	1. Technology in our lives
3	2. Cybersecurity - the security of technology
4	3. Nuances of Cybersecurity
5	4. Cybersecurity approaches
6	5. The human link
7	6. Action pillars
8	Social Considerations
9	Essential Ideas for IMPETUS Users
	Cybersecurity for Smart Cities
10	1. Levels of integration
11	2. Protection mechanisms
12	3. High level and horizontal synchronization
13	4. Specific vulnerabilities and threats
14	5. Essential lines of action
	Context for Future Adaptation
15	1. Perspectives for technology evolution
16	2. Glimpse on the evolution of cybersecurity risks
17	3. Needs for adaptation
18	Regulations Related to Cybersecurity
19	Cybersecurity Library
20	Cybersecurity Checklist for Smart Cities

Reading suggestions for Regulators

#reading_order	Section/ Chapter
1	Essential Ideas for General Users
	Principles of Cybersecurity
2	1. Technology in our lives
3	2. Cybersecurity - the security of technology
4	3. Nuances of Cybersecurity
5	4. Cybersecurity approaches
6	5. The human link
7	6. Action pillars
8	Social Considerations
9	Essential Ideas for IMPETUS Users
	Cybersecurity for Smart Cities
10	1. Levels of integration
11	2. Protection mechanisms

12	3. High level and horizontal synchronization
13	4. Specific vulnerabilities and threats
14	5. Essential lines of action
	Context for Future Adaptation
15	1. Perspectives for technology evolution
16	2. Glimpse on the evolution of cybersecurity risks
17	3. Needs for adaptation
18	Regulations Related to Cybersecurity
19	Cybersecurity Library
20	Cybersecurity Checklist for Smart Cities

Reading suggestions for Civil Servants

#reading_order	Section/ Chapter
1	Essential Ideas for General Users
	Principles of Cybersecurity
2	1. Technology in our lives
3	2. Cybersecurity - the security of technology
4	3. Nuances of Cybersecurity
5	4. Cybersecurity approaches
6	5. The human link
7	Social Considerations
	Cybersecurity for Smart Cities
8	4. Specific vulnerabilities and threats
	Context for Future Adaptation
9	1. Perspectives for technology evolution
10	2. Glimpse on the evolution of cybersecurity risks
11	Regulations Related to Cybersecurity
12	Cybersecurity Library

Reading suggestions for Regular Citizens

#reading_order	Section/ Chapter
1	Essential Ideas for General Users
	Principles of Cybersecurity
2	1. Technology in our lives
3	2. Cybersecurity - the security of technology
4	3. Nuances of Cybersecurity
5	4. Cybersecurity approaches
6	5. The human link

7	Social Considerations
	Cybersecurity for Smart Cities
8	4. Specific vulnerabilities and threats
	Context for Future Adaptation
9	1. Perspectives for technology evolution
10	2. Glimpse on the evolution of cybersecurity risks
11	Regulations Related to Cybersecurity
12	Cybersecurity Library

Reading suggestions for general users

#reading_order	Section/ Chapter
1	Essential Ideas for General Users
	Principles of Cybersecurity
2	1. Technology in our lives
3	2. Cybersecurity - the security of technology
4	3. Nuances of Cybersecurity
5	4. Cybersecurity approaches
6	5. The human link
7	6. Action pillars
8	Social Considerations
9	Essential Ideas for IMPETUS Users
	Cybersecurity for Smart Cities
10	1. Levels of integration
11	2. Protection mechanisms
12	3. High level and horizontal synchronization
13	4. Specific vulnerabilities and threats
14	5. Essential lines of action
(optional)	Cybersecurity Crisis Management
15 (optional)	1. Incident management
16 (optional)	2. Cooperation and reporting
17 (optional)	3. High availability
18 (optional)	4. Operational landmarks
	Context for Future Adaptation
19	1. Perspectives for technology evolution
20	2. Glimpse on the evolution of cybersecurity risks
21	3. Needs for adaptation
22	Regulations Related to Cybersecurity
23	Cybersecurity Library

Cybersecurity: Quick Intro



The essential ideas in relation to Cybersecurity principles and social considerations are summarised in the presentation below. More details are presented in the pages which follow.

The section is suited for:

- all audiences



D6.2 - Cybersecu..._quick intro.pdf

Principles of Cybersecurity



This section offers a general perspective on Cybersecurity, framing the topic in the overall image of security requirements related to technology. It also contains principles and good practices to be followed, in order to set a proper cyber hygiene among the Smart City users.

The section is suited for:

- all audiences

1. [Technology in our lives](#) - an introduction to the technological context
2. [Cybersecurity - the security of technology](#) - an introduction to Cybersecurity
3. [Nuances of Cybersecurity](#) - a summary of the facets of Cybersecurity domain
 - 3.1. [Technical cybersecurity](#)
 - 3.2. [Complementary cybersecurity](#)
 - 3.3. [Extensive coverage](#)
4. [Cybersecurity approaches](#) - common best practices in the applied field of Cybersecurity
 - 4.1. [Compactness and robustness](#)
 - 4.2. [Multi-layered protection](#)
 - 4.3. [Integration](#)
5. [The human link](#) - the role of human in the cybersecurity chain
 - 5.1. [Knowledge and expertise](#)
 - 5.2. [Trust](#)
 - 5.3. [Improvement and calibration](#)
6. [Action pillars](#) - main measures to be taken to create a cybersecurity foundation in a technological ecosystem
 - 6.1. [Complete implementation](#)
 - 6.2. [Standing by procedures](#)

1. Technology in our lives

This chapter comprises an introduction to the general tech environment, with an emphasis on the place and role of technology in our lives.

The chapter is suited at least for:

- Intelligence analysts
- Government staff
- Decision makers
- Policy makers
- Regulators
- Civil servants
- Regular citizens

Digital and emerging technologies are becoming more present in our daily lives, both in the physical environment and in the virtual space that supports our evolution and comfort. Everything around us seems to be more automatic, responding to our needs in customized manners and in real-time. Many of the private and social areas receive technological improvements, offering us a broader spectrum of choices at our disposal, in order to personalize our experiences and to increase our well-being.

In the same time, technology conditions us to some extent, since it creates the appropriate context for a new kind of risks (i.e., cyber risks) to arise and manifest, predisposing us to harm and losses. Every modern, high-tech environment that we create also has its shortcomings, which we need to treat accordingly in order to prevent and counteract any undesired related outcomes.

The current and future technologies that shape our social and physical environment increase the level of interconnectedness and complexity, and contribute to production of large amounts of data that map our actions and traits.

The digital social organization (i.e., information technology systems, networks, communications, services, etc.), as well as the digital footprints (i.e., data), offer a generous playground for hackers to express their destructive and exploitation intentions. More so, unintended harmful effects may be generated by technology on individuals, society and environment, as a consequence of wrong development, misconfiguration or misuse.

As a general behavior to be followed at individual, organizational and social levels, we need to pay attention to both sides of technology – i.e., good and bad – by compensating the enjoyment of its benefits with explicit efforts of risk management. The permanent vigilance related to the harmful side of technology helps us all to proactively avoid malicious incidents, thus maintaining safe and proper conditions for life, work, well-being and evolution.

2. Cybersecurity - the security of technology

This chapter comprises an introduction to Cybersecurity, as a domain of study and practice, underlining its importance as a fundamental feature for the entire life cycle of technology.

The chapter is suited at least for:

- Intelligence analysts
- Government staff
- Decision makers
- Policy makers
- Regulators
- Civil servants
- Regular citizens

Technology has two main features – functionality and security – that need to be developed equally and embedded intrinsically, in order to ensure stability in operation. The high rise of the malicious interests and activities in the virtual world poses any technological asset to risk, regardless of its place and purpose, thus making **security** a compulsory attribute to be implemented in the entire life cycle of the asset, from scratch to scrapping.

Then, the high interconnection of technologies forming the current and future Smart environments – e.g., the Internet, specialized or commercial IoTs, the merging between IT and OT, Artificial Intelligence, 5G and other high-rate communications, the human-tech integration – creates the context for shared risks, making each of the components to be responsible for the security of the entire ecosystem. More so, Smart environments create bridges between physical and virtual worlds, making it easier for the risks to emerge, adapt and scale in an unbounded fashion, leveraging on all the characteristics and vulnerabilities of the cyber-physical realm (which can be specific either to the physical/ virtual sides alone, or to their blending).

Security is a feature that needs to be implemented in all the technology life cycle stages, namely: research, design, production, regulation, use, influence/modeling, update/improvement, and scrapping. Depending on the specificities of each of the stages, security may consist of multiple forms of expression: research and design may develop security concepts, mentalities and architectures; production needs to build functional security features, mechanisms and controls; regulation may set security principles, rules and standards to be followed; deployment and use of

technology are prone to security experiences; the influence that technology brings on human, society and environment needs to be analyzed and managed according to a set of sanity and balancing criteria; and the scrapping needs proper security procedures, at least for data and environment protection.

3. Nuances of Cybersecurity

This chapter comprises a summary of the facets of Cybersecurity domain, covering both the technical aspects, as well as the social/humanistic ones that derive from the use and influence of technology in our lives.

The chapter is suited for:

- all audiences

Security of technology – or, **Cybersecurity** – consists in the optimal implementation of specific requirements, in a holistic way (across all the technological life cycle stages), to ensure an extensive state of safety and protection for all the parties involved in technology's existence and functioning: the humans, the environment and the technology itself. Cybersecurity is a multi-lateral field of study and practice, that encompasses both technical aspects, as well as complementary ones.

3.1. Technical cybersecurity

Technical cybersecurity is in direct relation to technology's main purposes of existence. The production, management and use of systems, as well as the regulation, policies, rules and procedures supporting development and deployment of systems (at any level, be it organizational, national or of any other kind), are all meant to ensure the implementation of the functionality for which technology has been created [Popescu, 2021, pg. 56-126].

3.2. Complementary cybersecurity

Complementary cybersecurity compounds all the collateral aspects, that emerge from the existence of technology, such as: the influence brought on human, society and nature; the changes in the social landscape (in terms of education requirements, or workforce evolutions); the criminality arisen from the use of technology (cyber-dependent and cyber-enabled crimes); the judicial implications at social level (e.g. in relation to human rights) and at individual level (e.g. in relation to personal data and privacy); the changes brought by digital transformation; the implications of the human-tech integration, a.s.o. These facets need to be considered and approached accordingly (in all the technological life cycle stages, as well), to ensure a proper control on the subtle effects that technology may have as a consequence of its use [Popescu, 2021, pg. 127-162].

3.3. Extensive coverage

The two sides of cybersecurity cover a wide spectrum of security mentalities that need to be managed correlatively, in the context of Smart City architectures and phenomena.

The rationale around systems and networks security architectures, desirable human behavior and supportive organizational procedures is covered by the technical side of cybersecurity, which describes direct protection mechanisms. They are approached in the current documentation, the Cybersecurity Framework.

The considerations related to protection of human rights and other correlated ethical issues are approached extensively in [Ethics and Privacy PG](#), and only tangentially in the current documentation.

The landmarks of evolution of technology are covered by internal deliverable *Envisioned evolutions of the operational environment*, and are approached from a security perspective in the current documentation.

4. Cybersecurity approaches

This chapter comprises common principles and best practices in the applied field of Cybersecurity, to ensure a unitary minimum level of protection of the technological networks.

The chapter is suited for:

- all audiences

In the context of high interconnection of devices, systems and networks, the component with the least level of cybersecurity becomes **the weakest link** in the overall technological architecture, putting the entire ecosystem in danger, through its predisposition to be exploited by the attackers as an access point to other assets of interest.

4.1. Compactness and robustness

The level of cybersecurity is dependent on the **compactness and robustness** of the measures meant to reduce the attack surface of the protected assets.

Compactness consists in finding the proper balance of measures that would ensure an optimal level of protection. Due to the high complexity of the technological ecosystems, too abundant security measures may become less efficient, thus generating waste of investment. Too few measures may also result in a low level of security, due to a lack of coverage of the vulnerable points, thus leading to exposure in front of attacks.

There is a Gauss curve that describes the balance of the cybersecurity protection level depending on the complexity and abundance of the overall measures taken. In these terms, the optimal cybersecurity is achieved in the context of sufficient protection measures (somewhere in the middle, not too many, not too few), implemented adaptively and customized in such a manner to serve strictly the requirements identified in the risk assessment processes.

The attack surface is the sum of the vulnerabilities that can be exploited by the attackers to penetrate the systems or communications, allowing them to move and manifest afterwards, at the level of the network.

4.2. Multi-layered protection

Compact security may be obtained by means of holistic approaches that seek to protect all the intrinsic and contextual levels of technology, in a logically correlated manner. Defense-in-depth [Popescu, 2021, pg. 86], Zero-trust model, Software Defined Perimeter are examples of the most robust models that offer fluent workarounds to ensure extensive protection of the technology.

Firstly, technology needs **protection at all layers**, starting with the physical perimeter (where the hardware equipment is hosted) and the procedural controls (that ensure the mapping of human actions on technology requirements), to the software levels of organization, such as: IT&C, OT (operational technology) and ETs (emerging technologies). All the cyber-physical components of technology need to be taken into account, all-round, especially in the cases of the on-premises infrastructures, with proper rules for network separation depending on the level of the assigned criticality.

Then, firm rules for **software-level management of security** need to be implemented – especially for the on-cloud services – in order to properly protect the communications and remote service platforms from any harmful tools meant for automatic discovery and penetration. Identity-based and role-based protection mechanisms (that allow users to access resources only according to their real identity and purpose/ need-to-know allowance) ensure that complex interconnected systems keep the functionality safe and shielded against unauthorized access.

4.3. Integration

Smart City fundamentally needs an **integrated approach** on cybersecurity, with a focus on implementation of compact built-in security and on ensuring real-time incident prevention and reaction capabilities [Pradhan, 2019].

Smart City environments compound all kinds of technologies (IT&C, OT, ETs), that are interconnected in complex logical architectures (at both hardware and software level) functioning in a wide variety of locations and contexts. The specific attack surface is vast and difficult to assess, making cybersecurity dependent not only on technical and administrative measures, but also on multi-layer cooperation and synchronization. Horizontal, seamless coordination of security operations is paramount to ensure protection of people and assets in case of cyber incidents.

5. The human link

This chapter depicts the role of human in the cybersecurity chain, underlining the need for knowledge and expertise, trust, and continuous improvement and adaptation.

The chapter is suited for:

- all audiences

5.1. Knowledge and expertise

Human is the most important factor in the entire cybersecurity life cycle. Beyond all the perfection of the measures taken to secure technology and organizational processes, the presence of human can strengthen or weaken the robustness of the cybersecurity status of the protected infrastructures.

As with any process, cybersecurity needs knowledge and expertise to be properly implemented, configured, maintained, deployed and managed.

Specialized competences are paramount for achieving an optimal cybersecurity level of the protected technology. Security thinking needs to leverage all the corresponding particularities and specificities of the physical and technological environment, in an adapted and customized manner, in order to completely harness the investments made for this purpose.

In the same time, **general and on-the-job awareness** related to cybersecurity is key to avoid accidents and undesired happenings generated by mistakes, negligence, and other kinds of unintentional human behavior that may endanger all the efforts consumed for security.

5.2. Trust

More so, **proper management of human relations** with own and contractual personnel is required, in order **to prevent and counteract any situation of inside jobs**. Even though this is rather a management issue, than a cybersecurity one, in practice, inside jobs are one of the most

damaging threats an organization can face in terms of cybersecurity. At least in the critical industrial sectors or critical infrastructures, some cautionary actions need to be carried out in these regards, such as: conscientious background checks (prior to employment), two-factor validation approaches (during activity) and safe disconnection from services and accounts (when necessary or at the job endings).

5.3. Improvement and calibration

Human presence, knowledge and decisions are the backbone of cybersecurity. They need to be focused on **prevention and counteraction** of cyber risks, in a proactive manner. A high level of situational awareness, and well configured and tested technical capabilities, should be able to prevent the occurrence of the most mainstream cyber incidents, as well as to warn in early stages and react in real-time to any eventual cyber-attacks that would pass by the outer security perimeters.

Ideally, cybersecurity would need **predictive capabilities** able to dismantle all the vulnerable conditions that favor the occurrence of cyber incidents. But, while this is only a theoretical desiderate (at least from technical perspective), human presence may facilitate the prediction of cyber events by the means of suited knowledge, experience, intuition, Intelligence, threat hunting and other humanly methods and tools.

6. Action pillars

This chapter presents the main measures that support the creation of a solid cybersecurity foundation in a technological ecosystem.

The chapter is suited at least for:

- SOC operators
- SOC supervisors
- IT personnel
- Intelligence analysts
- Government staff
- Decision makers
- Policy makers
- Regulators

Any technological architecture needs a set of measures to be taken to ensure proper implementation, monitoring and improvement of cybersecurity status. The plethora of corresponding measures revolve around the three following principles that describe the general conditions for a contiguous and functional cyber ecosystem.

6.1. Complete implementation

Security is not a patch to be attached to products, but an inherent feature. There are also stages in the technological life cycle when security is patched, but it is done only as an ultimate option to cover unforeseen vulnerabilities.

Security is best implemented from scratch, starting with the phases of design, research and development. **Built-in security** (or **security by design**) ensures robustness and compactness, offering technology an indispensable root layer of protection from the discovery and penetration actions done with malicious purposes.

Then, all the other stages in technology's life cycle need to be approached diligently and consciously from a security standing point, in order to avoid weaknesses and loose ends. The physical context, the hardware architecture, the software configuration, the communication channels, the deployment and operation actions, as well as the decommissioning, need security implemented alongside the base functionality. Reaching and maintaining key performance indicators of technology are dependent on the responsible implementation of security measures, as fundamentally as possible.

6.2. Standing by procedures

Apart from the technology-related measures, human behavior is paramount for leveraging on all the efforts invested in security. **Firm rules** need to be created around the deployment, use and maintenance of technology, and a **due diligence** awareness needs to be developed with respect to both on-the-job responsibilities and the overall organizational rigors.

All the organizational security rules and workflows need to be assimilated by the employers and contractors, to ensure protection of the entire technological supply, management and use chain, and to allow **coordination and integration of efforts**.

Knowledge and exercising (i.e., **education, training, exercising**) around the procedures are mandatory, in order to test and confirm the validity of the envisaged policies and controls, as well as to discover the flaws and the requirements for improvement and update.

Organizations – as high-level beneficiaries and managers of cybersecurity – need to take account of human predispositions and behavior, in order to prevent and limit any risk that may come from the inside of the technological ecosystem (be it proprietary or collaborative). A series of **human risk clearance measures** – e.g., background checks, two-factor management of critical infrastructures, procedural checks and balances, critical-job redundancy – can contribute to ensuring uninterrupted and performant functioning of services.


6.3. Unitary action

Timely prevention and reaction are accomplished through **synchronization of all actors and capabilities** responsible for cybersecurity. First of all, **management buy-in** is mandatory for a correct understanding, development and administration of cybersecurity requirements at organizational level, since it impacts not only the local security, but also the protection of the entire adjacent technological and commercial ecosystem.

Then, all the technical and human related **measures need to be integrated** from an actionable standing point. Information needs to be correlated and proactively shared among the stakeholders, in order to limit the spread of newly discovered vulnerability points. Collaboration on cybersecurity management facilitates the reduction in the attack surface of the in-house and shared infrastructures. And operational cooperation ensures quick reaction (containment, counteraction, recovery) to the on-going cyber-attacks.

Above all, **unitary decisions mechanisms** (e.g., pyramidal [CERT/CSIRT](#) structures) should be established and tested, to ensure proper response to cyber incidents. Cybersecurity efficiency is provided only if prevention and reaction capabilities have a dynamic at least comparable to that of the attackers.

Social Considerations

 This section offers information related to social considerations needed for a holistic approach of Cybersecurity, beyond the technical and operational sides of the matter. Individual behavior, due diligence, bureaucracy, judicial implications, digital competences, data management and protection, ethics and privacy, all shall be taken into account consciously and responsibly - apart from the technical efforts - to contribute to the overall state of cybersecurity.

The section is suited at least for:

- Intelligence analysts
- Government staff
- Decision makers
- Policy makers
- Regulators
- Civil servants
- Regular citizens

Diversity of cybersecurity

Cybersecurity is more than just the technical configuration of equipment. It is a series of conditions meant to ensure an overall state of safety for humans and nature, in relation to the use of technology. Simple life facts (that sometimes may even seem not correlated to cybersecurity at all) may represent factors that can endanger security of the cyber-physical environment without knowledge and track.

For example, a data leakage from a tertiary service (that has nothing to do with urban facilities) may offer to hackers a key for entering Smart City systems or for exploitation of personal data that are directly linked to public administration. This could be happening as a consequence either of misconfiguration of systems, or of human (unintentional) errors.

Or, an eventual gap in accountability over specific security responsibilities between two parties (e.g., due to inadequate contractual provisions) may leave unprotected areas – in terms of technology, processes or humans – which hackers would exploit unrestrictedly, since no one is in charge to take action for preventing and counteracting those associated risks.

Or, some fraudulent activities conducted in cyber-physical world may not be legally held accountable due to mismanagement or altering of evidence chain, or to a lack of regulation provisions that should incriminate those specific type of activities.

At first sight, these may seem soft problems, that can be fixed by simple decisions or by adjustment of social bureaucracy. They tend to be left out of cybersecurity discussions or receive a lower priority, the main efforts being concentrated on the development and deployment of security technology. But, in essence, they may pose serious challenges in the security context, since they can create social effects that cannot be reversed and also need longer times to be adjusted for reinforcement of the general eco-system's robustness.

Cybersecurity is a complex techno-social phenomenon that needs all-round provisions and actions which would evolve synchronously. The **complementary cybersecurity** provisions come to consolidate the *processes* and *humans'* sides of the digital eco-systems, offering the tools for a balanced development of the overall security of Smart Cities and to society in general.

Individual and collective decisions need to be aligned to technological society we live in. Judicial and administrative systems (including organizational policies and procedures) need to be adapted so as to incorporate provisions related to the common use and presence of technology in our lives. Bureaucracy needs to be updated and aligned to digitalized environments and services. Education needs to consider technology as a domain of study and to approach it both explicitly (in a dedicated manner), as well as implicitly (in correlation with other subjects /topics).

More detailed information on how to approach Cybersecurity in relation to specific humanistic topics may be found in [Library/ Documentation related to social considerations of Cybersecurity](#).

In particular, an overall image on complementary aspects (including social considerations) of Cybersecurity may be found in [\[Popescu, 2021\]](#).

As well, information related to the application of Cybersecurity in different social domains at EU level may be found in [Regulations related to Cybersecurity](#).

In a similar direction, [Ethics and Privacy PG](#) describes considerations related to the social implications of technology, with a focus on Smart City contexts.

Managing Cybersecurity: Quick Intro



The essentials of managing cybersecurity (Cybersecurity for Smart Cities, Cybersecurity Crisis Management, and Context for future adaptation) are summarised in the presentation provide here. More details are provided in the pages which follow. The material also presents some details of the IMPETUS approach.

The section is suited at least for:

- SOC operators
- SOC supervisors
- IT personnel
- Intelligence analysts
- Government staff
- Decision makers
- Policy makers
- Regulators



D6.2 - Cybersecu... quick intro.pdf

Cybersecurity for Smart Cities



This section depicts the specificities of cybersecurity relevant for urban environments that dispose of complex technological networks and services. It underlines the main approaches and mechanisms to be deployed in order to ensure a unitary cybersecurity and strong cyber resilience in Smart City eco-systems, while pinpointing the role of the IMPETUS tools in this context.

The section is suited at least for:

- SOC operators
- SOC supervisors
- IT personnel
- Intelligence analysts
- Government staff
- Decision makers
- Policy makers
- Regulators

1. [Levels of integration](#) - an integrated perspective on all the Cybersecurity requirements

1.1. [Facets of incidents](#)

1.2. [Technological perspective](#)

1.3. [Humanistic perspective](#)

2. [Protection mechanisms](#) - fundamental mechanisms to ensure Cybersecurity

3. [High level and horizontal synchronization](#) - requirements for collaboration on cybersecurity matters

4. [Specific vulnerabilities and threats](#) - a depiction of the main cyber vulnerabilities and threats

4.1. Understanding the incidents specifics

4.2. Threats

4.3. Vulnerabilities

4.4. Contextualizing incidents

5. Essential lines of action - a description of the main sets of cyber-related measures to protect Smart City environments

5.1. Human training

5.2. Automating technical capabilities

5.3. Leveraging human capabilities

5.4. Optimizing and customizing protection

5.5. Exercising and simulation

1. Levels of integration

This chapter depicts an integrated perspective on all the Cybersecurity requirements, including both the technical aspects and the humanistic considerations that emerge from the technology use and influence. The focus is put on principles that would ensure integration of efforts at a Smart City level.

The chapter is suited at least for:

- SOC supervisors
- IT personnel
- Intelligence analysts
- Government staff
- Decision makers
- Policy makers
- Regulators

1.1. Facets of incidents

Smart City is a complex technological environment that needs proper integration, in order to ensure **real-time synchronization** of actions for prevention and response to cyber incidents. The organization of protective measures in Smart City revolves around two basic approaches:

- Cybersecurity **in** Smart City – putting focus more on compactness and robustness of security in order to ensure protection against **cyber-dependent crimes and attacks**.
- Cybersecurity **for** Smart City – with a focus on implementation of specific security tools in order to ensure protection against **cyber-enabled crimes and attacks**.

Cyber-dependent attacks consist in the use of technology as both a means and a target for exploitation. They are generally focused on gaining access to technological assets (especially for data), in order to get leverage that can be used for further attacks or benefits. They may usually generate loss of money or data, but can also affect physical security in particular cases (e.g., encryption of data in hospitals for ransom can lead to human life damage or losses). Protection against cyber-dependent attacks is mainly based on **resilience of technology**.

Cyber-enabled attacks consist in the use of technology as a means to conduct classical crimes. Smart City is prone to malicious exploitation of technology for terrorism purposes, for example. Discontinuing water, energy or other utilities supply services directly affects masses of people, entire districts or cities. As well, attacks on digital public administration infrastructure may cause losses of financial assets, denial of critical services, access to health services, bogus changes on decision-making processes, etc. This kind of attacks pose direct pressure on people and social processes.

Protection against cyber-enabled attacks tends to be based more on **the behavior of people** and **compactness of processes**. Hackers usually seek to exploit human vulnerabilities (e.g., by the means of social engineering) and human social organization (e.g., by interposing in social flows or in supply chains), with the purpose to manipulate behaviors and decisions in such a way that would come to their final benefit.

1.2. Technological perspective

The digital ecosystem of Smart City may contain all kinds of technologies – from IT&C, to OT and ET – structured in network architectures both connected to Internet and isolated.

The administrative and business-as-usual networks, as well as the ones linking remote branches are, usually, connected to or over the Internet. The interconnectivity offered by the Internet creates the premises for quick **centralization and management of cybersecurity services** associated to the protected assets.

Nonetheless, the more sensitive and critical the technological network, the bigger the need to keep it disconnected from the Internet and other on-grid facilities. Industrial technology (e.g., **ICS/SCADA**) is often required to be physically separated from any other network and from the Internet, since it hosts critical services and data that need special, dedicated security measures. But any physical separation of networks leads to lack of unitary visibility and synchronization of cybersecurity operations, making the responsible **SOCs** lag behind in terms of prevention and reaction to cyber incidents.

The need for security integration becomes even more difficult to accomplish when considering also specific Smart City technology, which often consists in networks of distributed sensors that monitor critical assets/ networks/ services and need centralized management.

And last, but definitely equally important, the evolution of technology tends to create vast networks of interconnected and intelligent devices that are, basically, tools for unitary and coordinated peripheral implementation of centralized decision-making capabilities. These tools (the peripheral devices) usually have weak cybersecurity protection, since they are built from the start, due to functional and commercial restrictive requirements.

Artificial Intelligence over Internet of Things creates a broad network of distributed simple devices that can only act intelligently by following strategic instructions from the main server or cloud. The overall security of these kinds of systems are prone to exploitation due to the vulnerabilities residing in the edge devices (which play the role of the weakest links).

Integration of cybersecurity over a Smart City environment may be a difficult task. Though, there is a set of basic principles in relation to this purpose, that should ensure proper functionality of security services while maintaining operation of technology undisturbed:

- Cybersecurity centralization and management consists in **aggregation and processing of meta-data related to devices and network activity**, while leaving the main functionality of technology untouched. It is done by the means of dedicated services related to cyber events management and orchestration (such as **SIEMs**, **SOARs**).
- Internet connected networks may be fully centralized and managed from a cybersecurity standing point (unless specific local security requirements do not state otherwise). As an annotation, the cybersecurity integration should not affect any logical separation of networks envisioned in their functional architecture (which remains a paramount requirement for individual security of the protected services).
- The physically separated networks may be integrated in the overall cybersecurity architecture, but only ensuring one-way outbound flows of meta-data. This may be done using unidirectional systems for meta-data transfer (e.g., data diodes) at the edge of the network. Thus, the separated networks may be only monitored for situational awareness of cyber incidents. The incident management needs to be done locally (at the level of the protected network), via close cooperation with the centralized overseeing **SOC**.
- Cloud-based services (and especially ones that use networks of peripheral devices, i.e., IoTs) need to have proper security measures implemented in the core of the architecture, where all the data and intelligence reside. This does not exempt the peripheral devices from having their own security measures developed or implemented.
- Integration of meta-data needs deep correlation, processing and analysis, in order to allow a valid representation of the overall phenomena of the protected technological ecosystem. It needs to be done holistically, so as to reveal logic, human-readable information related to the existing cyber threats and incidents.

1.3. Humanistic perspective

Cybersecurity needs to integrate measures related both to **technology** (i.e., devices, infrastructure, communications, data), as well as to **processes** (i.e., organizational, commercial, industrial, urban) and **humans** (i.e., decisions, behavior), in order to ensure coherent and fluent flows of action. Alongside the technological approach, layering out security measures according to the humanly specificities consolidate the overall cybersecurity architecture, thus lowering the chances for cyber risks occurrence.

Considering the scale of its fundamental purposes (e.g., improvement of public services, digitalization of social services, facilitation of public-citizen interaction, ensuring environment protection, public security and safety, etc.), Smart City needs seamless correlation between all its functionalities with cybersecurity measures:

- Each purpose is accomplished by a set of corresponding services, that – in their turn – have rules of functioning, dynamics, technologies and impacted people.
- The services need to be holistically described and organized in a logical and unitary flow.
- Then, the services architecture needs to be mapped with the technological one, in order to identify the synchronization requirements that would allow early warning to cyber incidents and quick reaction times for their prevention and counteraction.

The more complex the Smart City environment, the simpler it needs to be represented in the cybersecurity architecture, so as to facilitate prompt decision making.

Cities are one of the most complex forms of human organization, posing a high challenge to physical security and cybersecurity. The protected targets need to be clearly represented by proper sensors (to offer explicit situational awareness), the technical analysis need to offer clear and certain information (to fundament the decision-making process) and the actions need to be firm, coordinated and efficient (to avoid or limit manifestation of risks).

2. Protection mechanisms

This chapter comprises of fundamental mechanisms to ensure Cybersecurity. It offers a more applied approach that helps building the security architecture of the managed network.

The chapter is suited at least for:

- SOC supervisors
- IT personnel
- Intelligence analysts
- Government staff
- Decision makers
- Policy makers
- Regulators

Cybersecurity in Smart Cities needs to be approached strategically, making use of instruments and mentalities that would simplify the understanding and the tasks needed to be done in the entire ecosystem. In the end, simplicity is complexity being organized and solved.

Apart from leveling the integration of networks, protection of Smart Cities from risks that can affect cyber-physical environment can be obtained by setting high-level mechanisms for management of cybersecurity, according to **specificities of the urban services**. Thus, cybersecurity measures need to cover domains such as: utility, public safety, transportation/ mobility, agricultural and environmental services, smart buildings, public Wi-Fi, administration, etc. [NIST, 2021]

Moreover, specific **high-level protection mechanisms** should ensure continuity of processes and holistic management of cybersecurity, throughout all the points and links that may contain/ represent cyber-physical vulnerabilities. The series of protection mechanisms shall include:

- **Edge security.** Implementation of security measures at the level of sensors or peripheral devices, in order to avoid physical and cyber tampering with. It is also highly recommended that their physical location to be known and managed in strictly controlled conditions.
- **Core security.** Strong resilience should be implemented in the cloud, servers and databases architectures where the main services, intelligence and functionality are hosted. For Smart Cities, it is especially recommended to ensure high-availability (HA), as well as full replication of resources in separate physical locations (for backup and redundancy).
- **Communications protection.** Along with edge devices/sensors and core computational structure, communications are one of the three main pillars of technological networks, that need to be thoroughly protected. This is ensured by measures such as: end-to-end encryption, physically separated and protected lines, redundancy in communications channels, DNS-layer security, access control rules and role-based management of resources.
- **Big Data management.** Data is the logical resource managed across the entire technological infrastructure. It is accessed, stored, processed, transported and registered in each device or server, and in the communication links. Cybersecurity explicitly protected confidentiality, integrity, availability, authenticity and non-repudiation of data. The high amounts of data generated by technology need proper protection and management at the level of both the useful content, as well as the meta-data (technical and Intelligence-based) used for security purposes. In the current and future perspectives related to Smart Cities, a high attention should be paid to the Big Data coming from municipal IoT networks and AI-based services, which need integration and normalized analysis for proper understanding, evaluation and substantiation of decisions.
- **SOC capabilities.** Security mechanisms are integrated and managed by the means of dedicated Security Operation Centers. The specialized technical capabilities offer SOC's the possibility to gain situational awareness and decision leverage, for proper prevention and reaction to cyber incidents. It is preferable to offer SOC's direct access for management of devices and networks, in order to block, stop, contain and remediate cyber-attacks in real-time. Where this is not possible (e.g. in the physically separated critical infrastructures), appropriate complementary/ alternate communications channels between SOC's and respective networks should be established, as well as frequently tested for high responsiveness and availability.
- **Unitary command and control.** Cybersecurity attacks are orchestrated by hackers to gain the malicious purposes with highest efficiency and in shortest time frames, while leaving behind as few traces as possible. The high complexity of Smart City environments reduces the capacity for quick security actions, exposing humans and assets to vulnerabilities, despite all the technical measures in place. Unitary command and control are paramount to ensure real-time security capabilities (both cyber and physical) that would be able to counteract the force and synchronization of cyber-physical attacks. It needs:
 - o to have a higher priority of action in face of the business-as-usual operation of the protected services;
 - o to be unanimously acknowledged and assimilated across the entire Smart City environment;
 - o to be properly documented (standardized by the means of organizational procedures) and periodically tested;
 - o to be thoroughly followed when is the case.
- **Knowledge.** A great proportion of security efforts shall be oriented towards education, training and exercising of human capabilities. General cybersecurity awareness needs to be formed in order to avoid unintentional incidents, while solid on-the-job and tech-related cybersecurity specializations need to be ensured at all levels of technology management in order to implement built-in security and proper capabilities for prevention and reaction cyber-physical incidents.
- **Ethics.** Beyond the main purpose of cybersecurity, which is related to ensuring proper conditions for technology functioning and for direct safety of humans, there are also collateral considerations related to the risks generated by the use of technology. The more (cyber)security technology and decisions are deployed, the more the humans' privacy may be mismanaged or violated, thus raising suspicions with regards to the efficacy and effectiveness of protection measures in place. There is a balance between security controls and privacy of people, that needs to be respected, in order to keep cybersecurity measures useful and relevant. [More details regarding the Ethics of technology is approached in [Ethics and Privacy PG.](#)]

- **General situational awareness.** Cybersecurity needs to make use of all tactics, techniques and procedures available to gain knowledge related to technological context/ environment and its generated effects. Technical sensors and equipment offer an understanding of the abstract cyber-physical playground; human Intelligence capabilities gather risk-related information from the physical/ human world and exposes all the cyber knowledge in a readable format for decision makers; trans-disciplinary research and analysis offers a perspective on the technological effects on humans, society and nature. All these processes are needed to integrate information in its most valuable and useful form, in order to substantiate decisions with regards to the development, use and security of technology.
- **Cybersecurity tools.** Dedicated tools for cybersecurity purposes cover all kinds of necessities, offering a plethora of functionalities, from prevention and detection of cyber-attacks, to documentation of malicious actions and environments, and to management of ethics requirements and situational awareness. Rather, customizing dedicated ones to fulfill explicitly certain purposes is a more reliable solution to implement, that would ensure also a proper use of the available resources. Considering the characteristics of Smart Cities, particular tools are mandatory to ensure proper prevention and reaction to cyber incidents, focusing on: cyber threats monitoring and detection capabilities, malicious activities and TTPs Intelligence deployment, integration of information and decision at SOC level, education of operators and specialists in cybersecurity domains, exercising and testing overall cybersecurity architecture and procedures, preparation for cybersecurity Crisis Management. In particular, IMPETUS offers a consistent part of these requirements by means of [Cyber Threat Intelligence/ CTI](#) and [Cyber Threat Detection and Response/ CTDR](#) tools, while managing them in an interoperable architecture, along with other physical security tools (such as [Bacteria Detector/ BD](#), [Workload Monitoring System/ WMS](#), [Evacuation Optimiser/ EO](#), [Urban Anomaly Detector/ UAD](#), [Social Media Detection/ SMD](#), [Firearm Detector/ FD](#), and [IMPETUS Platform](#)).

3. High level and horizontal synchronization

This chapter contains high-level requirements for collaboration on Cybersecurity matters, to facilitate the uniform implementation of measures and to exchange incident information.

The chapter is suited at least for:

- SOC operators
- SOC supervisors
- IT personnel
- Intelligence analysts
- Government staff
- Decision makers
- Policy makers
- Regulators

The [SOCs](#) of Smart City need to be integrated within the pyramidal structure of [CERT/CSIRT](#) entities that manage cyber incidents at national and international level, in order to facilitate counteraction of attacks that may be orchestrated at large scale. The multi-layer reporting scheme allows proper situational awareness irrespective of the ownership of the networks, thus serving properly to the overall/systemic security operational needs. Smart Cities represent critical infrastructures whose protection needs to be integrated as a part of national security.

More so, cybersecurity efforts shall be exchanged horizontally, among Smart Cities, as a collaboration to mutually support the prevention and reaction to cyber-attacks. Since the entire ecosystem's cybersecurity is dependent on the protection level of the weakest links, the responsibility for the overall state of protection is uniformly distributed among the participants to the local and national technological network. Exchange of information, reporting of events and incidents, reciprocal awareness related to the patching requirements, transfer of best practices, exercising and testing inter-platform direct cooperation, all contribute to the robustness of the entire Smart City environment, as a whole.

Hackers dispose of an exemplary collective organization and benefit from lack of rules and boundaries in relation to the targeted infrastructures, making attacks a very difficult challenge to overcome. On the other side, bureaucracy, laws, social rules, ownership and managerial implications, decision distribution, lack of clear visibility and understanding of activity inside the virtual space, the complexity of the technological environment, all these represent impediments that lower the efficiency of prevention and reaction to attacks. In these conditions, high level and horizontal cooperation are paramount for ensuring a proper defense against cyber threats.

4. Specific vulnerabilities and threats

This chapter depicts the main categories of cyber vulnerabilities and threats specific to Smart City environments. It also contextualizes the incidents that may arise and affect the protected infrastructures.

The chapter is suited for:

- all audiences

4.1. Understanding the incidents specifics

Cybersecurity measures are useful and efficient if adapted to respond specifically to the risks identified as most relevant for Smart City. Risk assessment processes explore the probabilities and the impact associated with the exploitation of vulnerabilities by certain threats, thus offering the premises for prioritization and management of risks according to their corresponding level of importance.

Knowing and understanding vulnerabilities and threats set the path for identification of an extensive list of possible cyber risks, that contain the most probable approaches used by malicious actors to initiate and conduct the attacks.

The good part in preparation for defense is that **hackers' mentalities and modus operandi** (TTPs – Tactics, Techniques and Procedures) **remain mostly unchanged**, in time. Understanding the adversary's "art of war" offers the chance to prepare a good prevention and reaction strategy that would ease the efforts for detecting and dismantling the main channels of attacks. An example and a starting point for deeper understanding of the subject is offered by MITRE ATT&CK, that builds relevant research on TTPs specific topics [MITRE].

The bad part is that **attackers' means and tools are continuously updated and improved**, making use of the highest tech capabilities in order to bypass the defense mechanisms and penetrate the targeted ecosystems. This may force the infrastructures' owners to build cybersecurity mechanisms capable of counterbalancing the level of high-tech threats, thus sometimes leading to a disproportion of value between the protected target and the investment for its security. To avoid these unbalances, different cybersecurity strategies may be deployed, that would capitalize not only on the available technology, but also on the expertise of specialized human resources, and on cooperation.

4.2. Threats

Threats to Smart City cybersecurity may come from:

- **Individuals and groups** conduct cyber-criminal activities to gain personal advantages (usually, economic) or fame. Similarly, to theft or fraud in the physical world, hackers focus on cracking systems and databases to get undue resources.

A particularly dangerous, and unique, category of harmful individuals consists in "the insiders", which are employees that, at some point in time, can turn against the organization with the intention to forcefully solve work conflicts or financial constraints, or with other purposes that may put people and environment at risk.

- **Terrorists and hacktivists**, which pursue gaining a manipulation on decisions (be them political, administrative or organizational). Similarly, to terrorism in the physical world, the attackers focus on leveraging mass fear to attract attention and force their will over the public decisions. Cyber-physical terrorism can affect human safety and health, as well as the availability of public services, thus leading eventually to serious disasters.

- **State actors**, seeking to gain strategic advantage over a metropolitan or nationwide population or resources. Usually making use of APTs (Advanced Persistent Threats) as tools for conducting attacks, state actors focus their efforts on cyber espionage, in order to get unauthorized access to confidential information that can facilitate disruption of societal processes and dynamics.

4.3. Vulnerabilities

Vulnerabilities of Smart City cybersecurity may consist of:

- Low built-in security, misconfiguration, negligent and improper administration, as well as lack of knowledge in the use of technology.
- Misconducting of ethical requirements in relation to technology; unbalanced security-privacy ratio that would result in abuses of people personal data and space.
- Poor protection and management of Big Data pools, especially of those containing personal data or operational/critical data.
- Poor setting of decision algorithms (e.g., based on AI technology) that may deliver unacceptable rates of false positives or false negatives. This may result in slow response to incidents.
- Leaving devices, services or entire network areas without protection, thus creating weak links or spots that can serve as backdoors to hackers for penetration and exploitation of the ecosystem.
- Misinterpreting, misassigning and mismanagement of the criticality to the protected infrastructure.
- Lack of cybersecurity knowledge and awareness at the decision making and management levels.
- Lack of cooperation, collaboration and synchronization on cybersecurity matters, among partners and competitors in the technological and social ecosystem.
- Lack of correlation and integration of cybersecurity efforts; lack of strategic perspective that would allow proper response to hybrid threats and asymmetric conflicts.
- Low cybersecurity education level of employees and population.

4.4. Contextualizing incidents

Cybersecurity incidents may arise either from unintentional events (e.g., happenings, accidents, negligence, lack of attention, lack of knowledge), or from intentional acts (i.e., attacks, crime). They may occur only in the virtual world (e.g., cyber-dependent crimes) or in the cyber-physical environment (e.g., cyber-enabled crimes), producing damages at a larger scale than in the case of classical/physical security incidents.

In the context of the high amounts of information that people need to manage in their daily lives, cybersecurity risks may be subtly emerging towards the domain of **disinformation**, propaganda and manipulation. Depending on the level of interest that the cyber attackers have, cybersecurity incidents may be transformed or used as a leverage for conducting **hybrid and asymmetric conflicts** that, in the end, may become a matter of national or community security (e.g., economic disruption, energy services DoS/DDoS, political/administrative decision tampering, social order destabilization, biohazards generation).

Threats and vulnerabilities need to be analyzed based on the local Smart City particularities and treated in an adapted approach in order to prevent and counteract the most specific set of risks in that environment.

5. Essential lines of action

This chapter provides a description of the main sets of cyber-related measures to protect Smart City environments, ranging from enhancement of human competences to improvement of technical capabilities.

The chapter is suited at least for:

- SOC supervisors
- IT personnel
- Intelligence analysts
- Government staff
- Decision makers
- Policy makers
- Regulators

There is a set of actions paramount for building proper cybersecurity conditions, focused on **preparation**, **prevention** and **reaction** to cyber-physical incidents.

5.1. Human training

Awareness and **specialization** of human resources accounts are at least half the investment that needs to be made in cybersecurity efforts. Understanding the technological functioning, as well as the relation between technology, human, society and nature, is mandatory for the ability to represent the accuracy of the activities happening in systems and networks, and in the attackers' circles. No technological architecture is able to express the analysis and the inferences that humans can do in relation to the security climate; it helps and supports the process, indeed, but human mind is critical for anchoring comprehension and decision in the realities surrounding us (a rationale that remains valid at least until the [Artificial General Intelligence](#) capabilities may arise – which is not supposed to actually take form until year ~2050, according to the average of predictions for the technological future).

5.2. Automating technical capabilities

A large proportion (which accounts, roughly, to 80%) of prevention efforts is done by **automation** of detection and blocking of cyber-physical incidents, using technological capabilities. These are usually focused on threat information management and consist of:

- *vulnerability discovery and patching*, making use of vulnerability scanning tools and follow-up remediation activities;
- *technical Intelligence gathering* (e.g., [Cyber Threat Intelligence/ CTI](#) tool) digging for threats in their forming phase, in order to support timely patching of systems and networks;
- *calibrated monitoring and detection* of incidents, using refined [SIEM](#) searching rules for specific threats;
- *comparison analysis* using registered [CVEs](#), searching for known threats that may still try to exploit unpatched vulnerabilities;
- *behavioral analysis* of systems and networks events and activities, searching for anomalies that would detect and prevent intrusions (which usually makes use also of AI and machine learning algorithms);
- *technical analysis* used for reporting and exposing the situation to the decision makers (operators and owners).

5.3. Leveraging human capabilities

Then, the automated processes are complemented by manual activities executed by highly specialized technical analysts, with the specific purpose of [threat hunting](#). These experts usually look for APTs and zero-day threats (that have not been discovered and registered anywhere yet), deliver patching recommendations to system administrators and share the information across the cybersecurity community, in order to timely reduce the newly discovered attack surface.

5.4. Optimizing and customizing protection


There needs to be a funnel representation from the totality of cyber-physical risks (both identified in the risk assessment, as well as existent in the real world) to the attack attempts, to the actual attacks bypassing the security mechanisms, and to the ones producing harm. The rate of filtering these attacks at each layer/phase of manifestation needs to be exponential, so that to reduce the harm-producing incidents to zero.

This desideratum may be accomplished by the means of **optimized response capabilities** (e.g., [Cyber Threat Detection and Response/CTDR](#) tool in IMPETUS), that would facilitate the work of rapid reaction and forensic teams, in managing active cyber-physical incidents.

5.5. Exercising and simulation

In order to have all the cybersecurity capabilities in good standing and ready to be deployed at maximum performance, **exercising and simulations** are required at the level of the personnel involved. Knowledge, skills, as well as procedures need to be tested and improved (when it is the case) by means of specific tools, direct collaboration in teamwork and high level (strategic and management) cooperation in roundtable exercises.

Cybersecurity Crisis Management

 This section summarizes the aspects to be considered for the management of cyber incidents, as well as of any eventual escalation of incidents into cyber crisis situations. It also reveals the necessary organizational/administrative requirements for ensuring optimum operational response to cyber incidents, in the context of horizontal synchronization (across the Smart City environment and with external partners) and vertical cooperation (with relevant authorities).

The crisis management considerations are then applied to IMPETUS context, pointing out the role of the proprietary solutions with respect to ensuring and supporting cybersecurity of Smart Cities.

The section is suited at least for:

- SOC operators
- SOC supervisors
- IT personnel
- Intelligence analysts
- Government staff
- Decision makers

1. Incident management - main actions to ensure a performant incident management process

1.1. Incident management stages

1.2. Events vs. Incidents vs. Crisis

1.3. Adjusting the perception

1.4. Adjusting the reaction

2. Cooperation and reporting - the role of cooperation for Cybersecurity implementation

2.1. The need for cooperation

2.2. Cooperation requirements

3. High availability - conditions to ensure continuity of services

4. Operational landmarks - a mapping with IMPETUS operational approach

4.1. IMPETUS Cybersecurity Mindset

4.2. Mapping the IMPETUS solutions

1. Incident management

This chapter presents the main steps to ensure a performant incident management process. It also provides landmarks for the correct definition of the situations that need incident management.

The chapter is suited at least for:

- SOC operators
- SOC supervisors
- IT personnel
- Intelligence analysts

1.1. Incident management stages

Incident management in cybersecurity is represented by the operational processes of preparation and reaction, having the explicit purpose of preventing and counteracting cyber-physical incidents. It includes a series of stages necessary for filtering and sorting the events, following a funnel triage methodology, in order to allow proper management of resources and measures taken for limiting the production of harm and damages, and to capitalize on the incidents' inertia that could offer the premises for documentation and dissemination of the threat information at the level of Smart City partners.

Incident management includes the following stages [NIST, 2012]:

- **Preparation** – which involves configuring and maintaining a resilient security infrastructure, raising human awareness and specialization in cybersecurity domain, management buy-in, exercising the response to incidents, improvement of weak points or leaks identified in the ecosystem.
- **Detection and analysis** – which implies usage of [SIEM](#) and [SOAR](#) capabilities for automated detection, as well as threat hunting processes, inside [SOCs](#), where funnel filtering and prioritizing, as well as thorough analysis are deployed in order to allow documentation of decisions for timely reaction to potential harmful incidents.
- **Containment, eradication and recovery**. The incidents that trespass the multi-level protection layers and manifest in the protected ecosystem need to be contained (in order to limit the harmful effects, to avoid spreading and to document their *modus operandi*) and eradicated (in order to clean the systems from the malicious code and actively operating threats). The affected assets need to be reinstated, to function seamlessly at the expected level of performance.
- **Post-incident activity** – which involves retaining evidence, as well as documentation, sharing and reporting information related to the occurred incidents, in order to support accountability, to substantiate decisions, to improve the ecosystem's protection and to increase the knowledge base with new lessons learned.

1.2. Events vs. Incidents vs. Crisis

There are differences in perception of concepts of "*events*", "*incidents*" and "*crisis*", when referred in relation to the physical world or to cyber space. The manifestation in the physical world is linear (bound to laws of physics) and traceable, while in cyber space it is rather scalable (dependent on human creativity) and transparent to the outside world. This makes events, incidents and crises have different dynamics depending of their place occurrence.

In the physical world, events and incidents are punctual materialization of accidents or human will, which usually is limited to specific areas, resources, time and inertia. The complexity of physical events and incidents is dependent on human capacity to organize, synchronize and manage in the physical environment, which – practically – has a linear scale of manifestation and may be easily identified, tracked, stopped and investigated. Once identified and neutralized the source of events and incidents, the propagation of manifestation is rarely out of control (e.g., when the disturbance propagates through ideas making neutral people adopt them and continue the implementation, more or less spontaneously).

In cyber space, events and incidents comport totally different meanings.

Events are all the technological activity inside systems and networks, recorded/registered as meta-data or logs, for functional and security purposes. Meta-data is a representation of the activity history inside the technological devices; almost any automatic process or human command is registered chronologically, in order to keep awareness and control over technology.

Cybersecurity events are logs with possible relevance for security purposes. Usually, they may be of the order of millions/billions per day, depending on the scale and activity of the technological infrastructure.

After thorough customized filtering, a small portion of events may represent potential cybersecurity incidents. Human technical analysis may conclude whether the identified incidents are a real manifestation of harmful activities or are just false positives. In parallel, threat hunting activities have the complementary purpose: to extract the false negatives from the neglected events (i.e., the ones that may have been perceived as irrelevant by the automatic filtering process, but are actually real incidents and pose assets to risk). Cybersecurity incidents may be of order of units/tens per day and most of them can be harmless, not being able to penetrate the protection measures to the core level needed for exploitation.

However, some cybersecurity incidents may be able to produce harm. More so, depending on the level of their complexity and the associated risks, cybersecurity incidents may generate situations of crisis, making it compulsory to synchronize the actions for a prompt response. **The differentiation between regular cybersecurity incidents and situations of cybersecurity crisis** is a matter of perception, categorizing and tagging, which is established and agreed by high-level decision makers in the preparatory phase, according to a series of specific criteria.

No less important is that Smart City consists of a cyber-physical environment, thus borrowing characteristics of both physical security, as well as cybersecurity. A crisis situation in a Smart City ecosystem may reflect occurrence of events and incidents in both physical and virtual environments, bringing leveraged harm and scaled consequences.

[Degraded Modes](#) section presents specific details related to the management of malfunctioning of, e.g., [IMPETUS solutions](#), requirements for building robustness and resilience of the infrastructure, as well as practical considerations for tagging and responding to cyber-physical crisis situations.

1.3. Adjusting the perception

Considering the high level of complexity characterizing Smart City environments, the managers of infrastructures need to keep their awareness updated and open, in order to calibrate their perception to the realities of the operational challenges. Threat intelligence and knowledge about the evolution of relevant risks need to substantiate the adaptation of events filtering and analysis, as well as the patching of the newly discovered contextual vulnerabilities.

Perception is paramount for gaining situational awareness. If it lags behind, the entire lifecycle of cybersecurity is delayed and weakened, making the protection efforts to be derisive. On the other side, it is very difficult to reach a perfect understanding of the environmental risks, due to lots of factors that overpass the human control (at least at the level of administrators and managers), e.g., physical limits of sensors, limited sets of data extracted from sensors, limits of hardware and software processing capabilities, countless but sometimes difficult options for integration and analysis of all the collected data.

However, **continuous improvement on adjusting the monitoring processes** helps manage the degraded operation of platforms, identifying the indicators of threat appearance, as well as envisioning and preventing the materialization of risks. It is an operational change management process, that allows continuous adjustment to the evolution of risks, in conditions of high dynamics and uncertainty.

Perception adjustment needs to be a requirement for the crisis management procedures, since it improves the preparation stage and helps approach normal incidents and crisis situations in a differentiated way. It is a management tool for setting the proper conditions and parameters that would allow an efficiency increase of the cybersecurity efforts and resources.

1.4. Adjusting the reaction

The managers of infrastructures need also to keep themselves alert, to allow the reaction capabilities to be deployed spontaneously in the event of a risk manifestation. All the stages of incident management process need to be seamlessly correlated and synchronized, in order to limit any potential harmful consequences.

The optimal implementation of incident management is dependent on **the quality and calibration of the procedures**, on **exercising and testing the reaction capabilities**, on **the creativity to respond to on-going incidents**, as well as on **the adaptation of procedures and the improvement of preparedness, knowledge base and expertise**. All the actions taken prior, during and post incident bring an added value to the reaction chain. Thus, they need to be improved, correlated and duly taken.

While the foundation for incident and crisis management consists in the preparation efforts, the actual success and efficiency stand in the capacity for spontaneous adaptation to the situation's dynamics. Procedures and exercising facilitate coordination and scaling of reaction, while creativity and expertise support suited tactical and strategic decision making.

2. Cooperation and reporting

This chapter emphasizes the role and specifics of cooperation for Cybersecurity implementation, and enlists the activities and IMPETUS tools that support the reporting activities.

The chapter is suited at least for:

- SOC operators
- SOC supervisors
- IT personnel
- Intelligence analysts
- Government staff
- Decision makers

2.1. The need for cooperation

In a multi-stakeholder context (e.g., Smart City), besides the proper preparation and deployment of security capabilities around each of the protected infrastructures, the most important actions to be done for **streamlining the incident management process** are reporting and cooperation. Synchronization of individual and orchestrated actions (i.e., between multiple **SOCs**) is needed to counteract the spreading of the malicious activities and to limit the harmful effects.

Usually, the attackers have an advantage – based on their lack of need to respect social laws/ rules/ procedures and on their high collective organization – that allows them to deploy fast and stealthy actions. The slowness of bureaucracy inside authorities, institutions and organizations needs to be compensated with **agile action paths**, to allow **real-time reaction** in front of complex attacks.

Each **SOC** shall have their own properly customized communication and action procedures in case of cyber incidents, that would allow firm reaction to keep the infrastructures in good standing. An emphasis is put around the fact that **cyber-physical resilience is dependent both on preparation actions, as well as on adaptation capacity**.

Then, **coordination among SOC**s shall be clearly established and tested, in such a manner that would allow horizontal cooperation, bottom-up reporting and top-down command and control, in non-overlapping conditions. **The distribution of responsibilities and the requirements for communication** shall be well established, in order to ensure proper information for decision substantiation and optimal workflows for decision implementation.

2.2. Cooperation requirements

Depending on the custom conditions of the protected technological ecosystems, the organization of **SOC**s communication shall be done in **the most advantageous architecture** that would ensure situational awareness, decision facilitation and support, as well as firm reaction to incidents. Usually, the **SOC**s structure is built up around **a pyramidal system-of-systems** that allows strategic management of security under unique/unitary command and control capabilities.

IMPETUS cybersecurity approach takes advantage of these principles to concentrate relevant information and technical tools under the command of a single **SOC** having the capability to deploy real-time reaction to incidents. System and sensory data, as well as Intelligence, is collected (e.g., mainly via automated tools, such as **Cyber Threat Intelligence/CTI** in IMPETUS), as well as processed and leveraged (e.g., via

correlation tools, such as [Cyber Threat Detection and Response/CTDR](#) in IMPETUS). Correct understanding and management of the operational information supports the situational awareness and the decision-making processes, thus being vital for preventing and timely annihilation the threats that endanger the safety of people in high-tech urban ecosystems.

Reporting and cooperation are supported by subsidiary activities such as:

- information collection (from sensors);
- Intelligence gathering (from both technical and human sources);
- information analysis and processing (by both technical and social analysts);
- transfer of indicators of compromise and [CVE](#) information;
- technical information exchange between operational teams and between [SOCs](#) (with the ones not related to Smart City/ IMPETUS);
- technical support for patching and remediation;
- informing operational decision makers, relevant stakeholders and infrastructure owners;
- informing the media and public (with relevant aspects, when it is the case);
- dissemination of lessons learned and best practices in the cybersecurity community.

All communications need to be done on corresponding channels, depending on the sensitivity of the information. Cybersecurity usually makes use of **dedicated communication platforms** (i.e., dedicated and secured chatting, forums, information exchange, e.g., [MISP](#) platforms), strictly following [TLP](#) protocol to respect the **need-to-know** and **need-to-share** principles.

More so, Smart Cities can also create their own **trusted cybersecurity communication infrastructures** (i.e., identity-based trust frameworks), to ensure interoperability, resiliency and coordination of security related actions. This may not only support Smart Cities cooperation, but also interconnect with other multi-purpose trust frameworks, to integrate cybersecurity of multiple industries at national and international level.

3. High availability

This chapter enlists the conditions to ensure continuity of services, and maps the IMPETUS tools that provide support in these regards.

The chapter is suited at least for:

- SOC operators
- SOC supervisors
- IT personnel
- Decision makers

The success of crisis management is measured by the capacity to **resist**, **confront** and **overcome** adversity, having in the end as few as possible damage (preferably none at all). Response to crisis consists in leveraging on the adaptation capacity of both cybersecurity technology and human decision in such a manner to ensure a proper **resilience** at the level of the entire protected ecosystem.

Cybersecurity incidents may occur at any time and are not limited to physical boundaries. They pose great pressure on the security mechanisms to be fully prepared and operational at any time. The **uncertainty** specific to cybersecurity threats manifestation generates the need to implement 24/7 operational [SOCs](#), with continuity personnel that can ensure **permanent monitoring and analysis** of the threat landscape.

In case of major incidents that trigger crisis situations, an **operational crisis management cell** shall be deployed in no time, to be able to react properly to the occurring events. This structure consists of high-level decision makers empowered to dispose appropriate action for the security of the entire Smart City ecosystem. All the relevant social actors shall be represented in the crisis management cell, to protect the people and technology prone to adversity.

In order to ensure high availability of the crisis management capabilities, **specific procedures** shall be developed and frequently tested. As well, **dedicated exercises** – both hands-on and table-top – shall validate the functionality of cybersecurity technology and the efficiency of operational cooperation and reporting mechanisms.

In these regards, IMPETUS offers the [Cyber Threat Detection and Response/CTDR](#) tool for processing and optimizing the response to possible cybersecurity attacks, and for calibrating the strategies to approach the particular high-probability Smart City-related threats that are identified by the means of the [Cyber Threat Intelligence/CTI](#) tool.

4. Operational landmarks

This chapter provides a description of IMPETUS approach with regards to the cybersecurity operational landmarks, emphasizing the logic of tools inside the [IMPETUS platform](#) and the security process flows that they support.

The chapter is suited at least for:

- SOC operators
- SOC supervisors

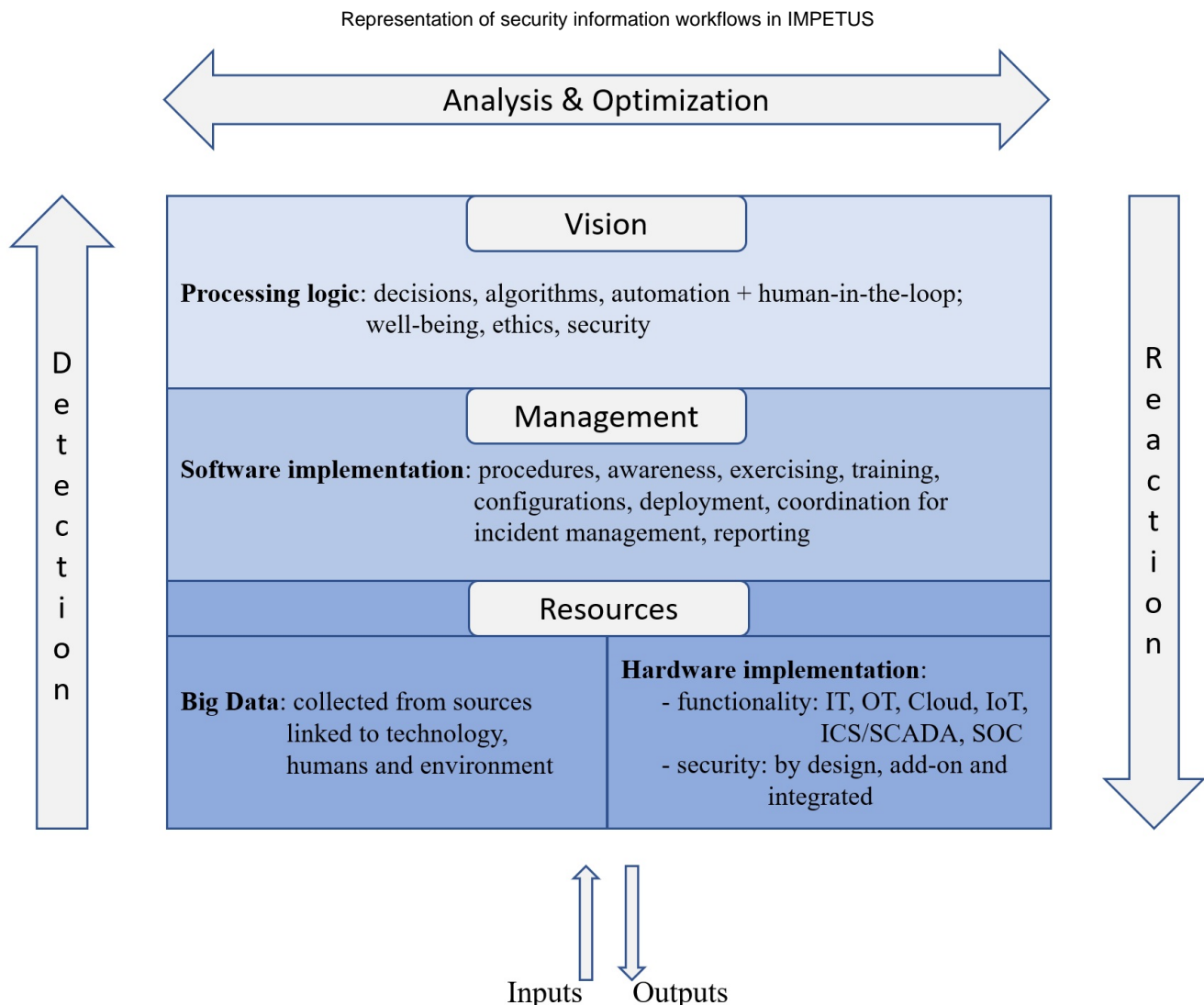
- IT personnel
- Intelligence analysts
- Government staff
- Decision makers

4.1. IMPETUS Cybersecurity Mindset

IMPETUS makes use of a series of cyber and physical security technologies that ensure the protection of Smart City environments. The security infrastructure consists of sensors, data collectors and transmitters, threat Intelligence gatherers, vulnerability detectors and assessors, information processing and analysis tools, simulators for exercising and training, as well as incident management solutions. These are all **managed in a centralized manner**, in a **SOC** with integrated monitoring and support for unitary decision, command and control.

The entire architecture benefits from **multiple layers of information processing**, thus allowing funnel filtering to extract the most relevant and accurate essence out of massive structured and unstructured databases (Big Data with open, functional, operational, Intelligence and security information). From data to decision, information is subject to multi-level analysis, in direct relation to the functional specifics of operators. Thus, the **IMPETUS platform** disposes of **dedicated view modes** for developers, administrators, analysts, security specialists, high-level **SOC** operators and decision makers.

A symbolic representation of the **security information workflows** of IMPETUS is envisaged in the figure below. Tools such as **Urban Anomaly Detector/UAD**, **Cyber Threat Intelligence/CTI**, **Social Media Detection/SMD**, **Firearm Detector/FD** and **Bacteria Detector/BD** facilitate data gathering from various sources in physical and virtual environments, **Workload Monitoring System/WMS** supports Big Data analytics and interpretation, as well as **Cyber Threat Detection and Response/CTDR** and **Evacuation Optimiser/EO** offer a solid ground for optimization of decisions and response, in order to prevent and counteract the cyber-physical incident and to avoid or limit any eventual damages.



4.2. Mapping the IMPETUS solutions

IMPETUS comes with a series of dedicated cybersecurity solutions (i.e., [Cyber Threat Intelligence/CTI](#), [Cyber Threat Detection and Response/CTDR](#) tools) that support information gathering, vulnerability analysis and response optimization.

[Cyber Threat Intelligence/CTI](#) offers the capability of automated search for threats in the deep and dark web environments, in order to extract the main characteristics of high probability attacks that can endanger Smart Cities in the foreseeable future. This kind of information has preventive relevance and shall prepare the administrators to properly patch the systems' vulnerabilities, as well as the security operators to focus their attention and analysis on newly found risk indicators (that have not been released publicly, as [CVEs](#), yet).

Threat intelligence offers the best preparatory lever for cybersecurity. Besides any of the detection capabilities, proper Intelligence (related to technical [TTPs](#) of attackers and to their human intentions and actions) ensures the basis for timely and precise decisions related to consolidation of security weaknesses. Networks are scanned for supposed vulnerabilities, detection mechanisms are calibrated on the newly malicious behaviors that are expected to occur in the systems activity, threat hunting is focused specifically on the indicators of the coming/predicted attacks, and new [CVEs](#) are born, to help protect Smart Cities from any cyber-criminal activity.

Knowledge related to future actions of hackers allows an increase in efficiency of security resources management.

[Cyber Threat Detection and Response/CTDR](#) uses facilities based on attack graphs to offer operators improvements and optimizations for response to cybersecurity incidents. It ensures a loop of learning that gathers experience and knowledge from incident situations, fusing and correlating data coming from multiple and diverse sources, and transforms them in applied modeling of the reaction capabilities.

The IMPETUS cybersecurity tools offer multi-layered awareness and protection, contributing to elimination of security weaknesses in the Smart City ecosystems. They use a holistic approach (which covers and tests all the technological assets and dynamics) to enhance infrastructure robustness and resilience, thus raising the capacity of prediction related to risks occurrence.

Context for Future Adaptation



This section envisages a set of cybersecurity requirements to be followed along the evolution of technology in Smart City environments. It focuses on maintenance of the safety conditions in the long-run.

The section is suited at least for:

- SOC supervisors
- Intelligence analysts
- Government staff
- Decision makers
- Policy makers
- Regulators

1. [Perspectives for technology evolution](#) - a depiction of the main trends for the evolution of technology

1.1. [At the applied level](#)

1.2. [At the information level](#)

2. [Glimpse on the evolution of cybersecurity risks](#) - a review of the main trends for the evolution of risks

3. [Needs for adaptation](#) - a set of high-level actions needed to manage the evolution of risks

1. Perspectives for technology evolution

This chapter depicts the main trends for the evolution of technology, with relevance for the Smart City environments, and a set of generic requirements to manage the corresponding impact.

The chapter is suited for:

- all audiences

In the rapid pace of technology's evolution, the changes of the social environment may become challenging. On the one hand, digital technology tends to evolve at a higher rate than the one needed by the human to adapt to changes (e.g., the quantity of information produced by the digital environment may sometimes exceed the human natural capacity to process and assimilate, thus leading to poor or misguided use of technology).

On the other hand, the complexity of some technological environments (e.g., Smart City ecosystems) can make it difficult to track and update all the functional and security requirements, which may lead to a lack of control over the overall image of the targets to be protected. Thus, unnoticed vulnerabilities may become weak links that can pose the entire chain of protection at risk.

Moreover, automation and autonomation predispose humans to lose control over technology (e.g., Artificial Intelligence designed to facilitate decision making processes may become a partial or a total black-box due to self-evolving algorithms). Lack of knowledge regarding the background processes generates uncertain effects, thus predisposing to a profound weakening of the security of the social realm.

Considering the high dynamics of technology's evolution, **the security mindset needs to follow a principled approach** that maintains its validity regardless of the particularities of any technologies that we may face in the future in any context of Smart City. Cybersecurity needs to offer a basis for proper adaptation, to keep technological eco-system safe and balanced in the long run.

As a general landmark, cybersecurity seeks to ensure optimal conditions for technology's functionality, serving both security and safety purposes (i.e., it considers both threats and vulnerabilities, in its efforts to manage the risks). The associated risks are facilitated by (and sometimes even dependent on) a series of **factors specific to the evolution of the technological and social landscape**, that may be shortly enumerated as follows:

1.1. At the applied level

- **Systemic complexity and sensory abundance** will continue to grow, especially in the Smart environments.

They impose robust and reliable architecture, clean implementation and focused attention to configuration. Management, performance and resilience of services depend on the quality of network partitioning, as well as on the accessibility to each of the technical facilities. Simplicity is solved complexity.

- **Interconnection and diversity** of the service delivery platforms (e.g., via IoT, 5G) will support fluency and customization of experiences.

They impose uniform and unitary protection of networks, to avoid single flaws and weak links. The development of an all-round compulsory level of security may require substantial effort, but it is also indispensable for maintenance of the proper functioning conditions of technology.

They also impose custom adaptations of security configurations to fit some particular/explicit needs, as well as raising awareness to involve humans (i.e., users, operators, managers, decision-makers etc.) as direct participants in the maintenance of security.

- **Interleaving between IT and OT** will make it difficult to discern between critical and non-critical infrastructures.

This imposes an adjustment on the perception of criticality both in terms of the level of granularity, as well as related to the associated scope.

IT and OT networks have different purposes and specificities, leading them to manage different sets of data having different needs of security. Any merging between the two imposes a strict definition and assignment of specific/separate measures for the proper management of the security requirements.

More so, the specialized terminology of "critical infrastructure" should be assigned not only to organizations, but also to industries or to similar complex ecosystems (e.g., Smart Cities, civil aviation, energy sector, e-government). To ensure a seamless and real-time protection of broad and heterogeneous technological environments having great importance for the community security or for the national security, the responsibility over cybersecurity needs to be assumed in the most extensive manner. Any weak point of protection may endanger the overall technological architecture.

- **Automation and autonomation** (e.g., via Artificial Intelligence) will empower technology with easiness of action and with decision-making capabilities.

As a general security requirement, people need to ensure they keep their control over technology and over the influence it has on its users and on the environment. Self-awareness and knowledge of technological background processes will be indispensable for maintaining proper human-technology interaction in the future.

1.2. At the information level

- **Information overload**, due at least to excessive data generated by equipment, increase of general human knowledge base, increase in customization of services and marketing activities, growth of digital disinformation.

It hinders the domestic/daily management of information, predisposing people to misguide themselves, to encounter difficulties in decision making processes, or to experience unconscious psychological adaptations. On a large scale, the abundance of information may generate subtle influences both in individuals and in society, leading us to unknown risks.

Also, the information overload may affect the operational processes, the technical analysis of data, thus lowering the capability to react and counteract the manifestation of risks.

- **Continuous novelties in technology landscape.**

Digital technology evolves at a rapid pace, forcing us to maintain a continuous effort of adaptation to its specificities. Cybersecurity cannot be set as a static/one-time state of protection; it must be updated and refined permanently, to be able to respond correspondingly to the changes that occur in the threats' realm. Cybersecurity requires a continuous effort for adjustment and improvement, as well as a correct perception and understanding at the management and operational levels, in this regard.

- **Overlapping responsibility**, due to multivalent fields of work and complex multi-industry phenomena (e.g., urban mobility via autonomous UAVs).

Some of the future technologies that will be deployed in the urban area may bring great challenges to the safety and security of the population. Autonomous UAVs, for example, will comport multi-valent risks (reaching from physical injury of individual people to disturbance of large urban /social assets) that need to be approached in unison by multiple authorities: the police, the local administration, the civil aviation authority, the national security authorities (e.g. in cases of terrorism) and maybe others.

Such complex phenomena need proper preparation and clear understanding of roles, to overcome difficulties in management and operation, and to reduce the reaction time to security incidents and crisis. Firm allocation and separation of responsibilities, as well as full coverage of the protection measures over the entire socio-technological realm, are needed to ensure unitary, relevant and efficient counteraction of risks.

- **Security vs. Privacy balance will be harder and harder to manage.**

The growth in the amount of usage data and personal information, as well as the complexity and customization of technology, make privacy management an increasingly burdensome mission for the security departments. Development of security culture and awareness at the level of the general population, and proper development of regulations, are paramount for leveraging on the security-privacy challenge in the best interest for the people.

- **Rapid evolution of the social landscape.**

The adoption of smart technology will change the way we interact and evolve in the social landscape, commuting from the classical understanding of the social life to a digital one. Influences and changes brought by technology to humans (and also to nature) need to be known, analyzed and understood, in order to support the decisions that will govern the long-term evolution of society.

2. Glimpse on the evolution of cybersecurity risks

This chapter provides a review of the main trends for the evolution of cybersecurity risks, with relevance for Smart City contexts.

The chapter is suited for:

- all audiences

The evolution of technology and society gives rise to a wide range of risks, related both to technical and non-technical aspects of our lives. Since much of our activity moves from physical to virtual space, the threat factors adapt and emerge, to exploit the continuously updating technological environment.

In a general note, we may observe that risks revolve around exploiting data and information, with a diversity of purposes ranging from economic to political ones. In this regard, we might need to take into consideration possible evolutions of threats and vulnerabilities relevant to Smart Cities, such as:

- **Frequent human errors**, that may result in misconfiguration and maloperation of equipment, mistaken data management, unintentional data leakage – that ultimately create weak links and points of access to Smart City data, services and tools (in general, not only related to IMPETUS);
- **Lack of overall knowledge and situational awareness** over the protected infrastructure and services. A complex and dispersed environment may be difficult to keep under complete supervision and monitorization, especially when having multiple owners.
- **Difficulty in drawing complete risk assessments**, due to the multitude and diversity of risk factors.
- **Lack of management buy-in**, due to a lack of understanding and perception of the practical cybersecurity needs.
- **Adaptive targeted social engineering**, which may be adjusted on-demand. Spear phishing may be easier to conduct due to the rich databases with users' personal data gained through customization services and preferences settings. Moreover, AI-based spear phishing may threaten all levels of users, regardless of their rank or job.
- **Partial or complete loss of human control** in the face of automated technology, that may lead to uncertain social effects in the future.
- **Disinformation**, that may generate a wide range of destructive effects, from confusion, information overflow, decision obstruction, to political maneuvers, economic imbalances and educational disparities.
- **Next-gen cyber warfare**, that can be conducted via the cyber-physical realm, with no borders, no time and resource limitations, and no liability over malevolent and destructive actions. It may seamlessly merge operations related to cyber domain, hybrid warfare, informational conflicts, economic manipulation and industrial disruption, to impose large-scale interests.

3. Needs for adaptation

This chapter offers a set of high-level measures and actions needed to manage the evolution of cybersecurity risks, with relevance for Smart City environments.

The chapter is suited for:

- SOC supervisors
- Intelligence analysts
- Government staff
- Decision makers
- Policy makers
- Regulators

Considering the high pace of technology's evolution, we need to deploy **agile adaptation** mechanisms, to permanently improve our understanding, capabilities and actions. The three facets of the societal realm – technology, people, processes – need to be managed accordingly, to ensure a safe and secure living environment in the Smart Cities:

- **Technology needs a secure lifecycle**, from scratch to scrapping, regardless of the dynamics in the changes that it suffers along the configuration, deployment and improvement stages;

- **People need awareness and direct implication** to the maintenance of security, regardless of their job or position in society;
- **Processes need to be openly and continuously adjusted** to support a seamless implementation of the operational requirements of security, regardless of their bureaucratic constraints and financial limitations.

There may be lots of **measures and actions** that contribute to the assimilation of technological progress. In the following, we mention some examples that can counterbalance the risks to cybersecurity of Smart Cities:

- Implementing **digital competence training** – both general, related to digital technology, and specific, on cybersecurity – that would form a baseline of knowledge for the population and workforce, with regards to the proper use of technology, and to the management of security risks.
- Setting **educational conditions for life-long learning** in the technological domains of expertise, to facilitate continuous adaptation to changes.
- Developing **open mechanisms** to assimilate the technological evolution at the social level and to adapt the judicial/official processes to the features of the new instrumental realities (e.g. set an appropriate ecosystem for adoption of autonomous urban UAVs networks).
- Continuous **update of the knowledge related to attackers' tactics, techniques and procedures** (e.g., [MITRE ATT&CK TTPs Matrices](#)).
- Improving and implementing **due diligence** with respect to security requirements, including:
 - o **Management buy-in and awareness** – to understand, take ownership and manage the technological phenomenon (both in terms of security needs and risks).
 - o Appropriate **investment for capability development** (both in terms of security equipment and development of specialized teams/personnel) and compliance with standards and certifications.
 - o Setting careful configuration and appropriate procedures, to maintain **cyber hygiene** both in the area of use/operation and to counter cybersecurity risks.
 - o Development and maintaining mechanisms for functional redundancy, data backup, and **readiness for crisis management**.
 - o Development of **two-factor high-level mechanisms to supervise and control** the proper functioning of smart technology (that involves automated decision management, e.g. AI), so that the error rate is kept at the lowest possible level, and the harmful impact on humans is negligible.
- Developing AI and Big Data processing capabilities, and **increase the degree of automation** that support human efforts of security.
- Developing, modeling and adapting **strategic approaches**, to comprehensively cover the management of technology and to develop unitary command and control capabilities able to prevent and counteract the materialization of security risks.
- Increase **common ground for operations** between agencies with direct interest for security (e.g. Municipalities, Police, National Security, [CERTs](#), [SOCs](#)), through shared representation of information. As well, proceeding to a safe integration in the community's security architecture of any siloed networks.
- Continuous improvement of mechanisms for **early detection and prevention** of security events.
- Developing, maintaining, updating and testing of the **trust chain**, so that systems and networks evolve in trustworthy and secure conditions, with vulnerabilities and attack surface diminished to the most extent.

Regulations Related to Cybersecurity



This section presents a mapping of the current regulation landscape applicable for Cybersecurity in Smart Cities (in the European Union), organized on the following topics:

1. [Technical Cybersecurity](#)
2. [Complementary Cybersecurity](#)
3. [Artificial Intelligence](#)
4. [Disinformation](#)
5. [Digitalization](#)
6. [Data, and Data Protection](#)
7. [Critical infrastructures](#)
8. [Practical guidelines for Smart Cities](#)

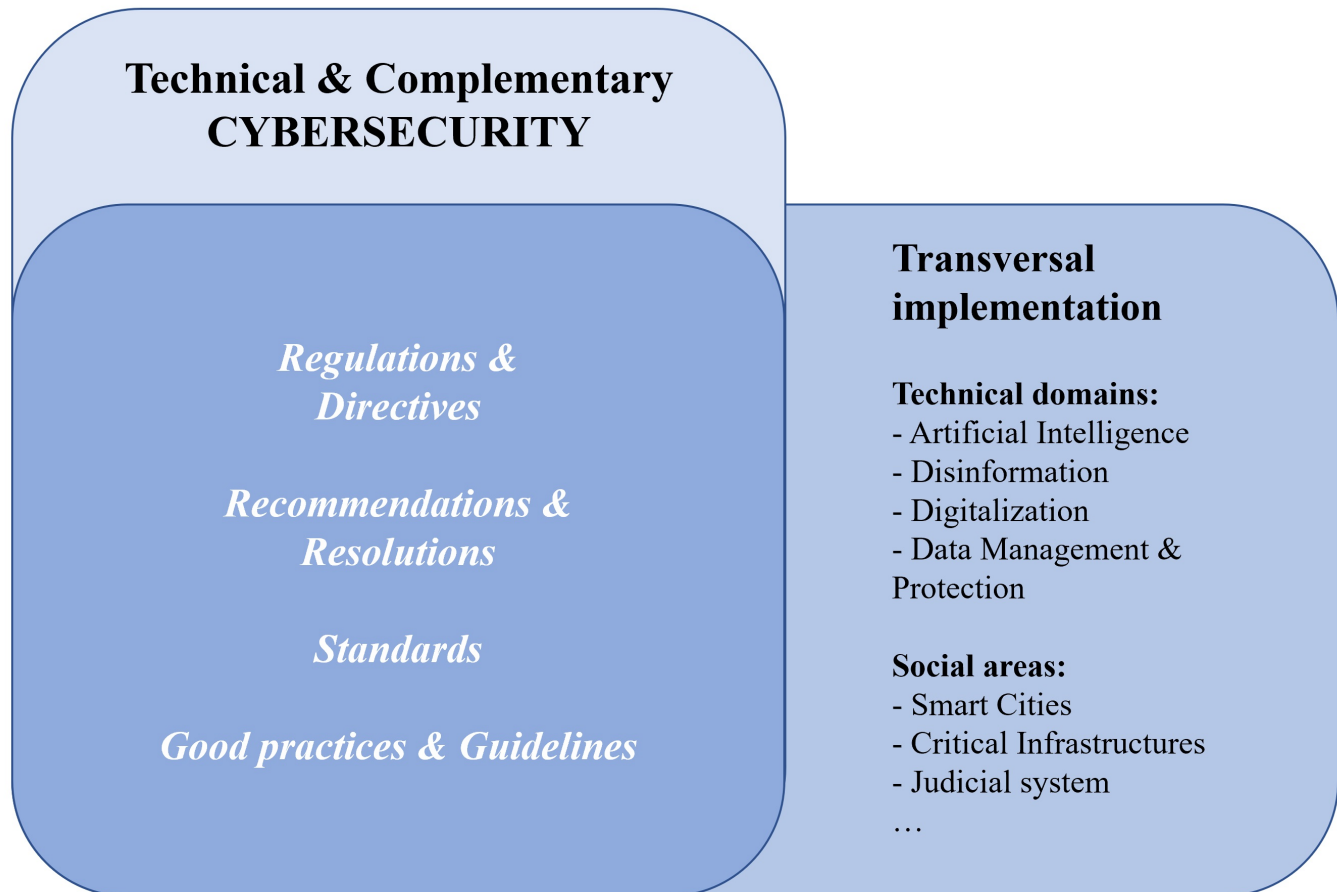
The section is suited for:

- all audiences

In 2022, the EU cybersecurity regulation landscape comprised mainly general cybersecurity provisions and secondarily industrial and emergent technologies specificities.

The regulatory acts or initiatives may be followed correlatedly depending on their targeted domain of practice in the *technical* spectrum (e.g., cybersecurity, artificial intelligence, digitalization, data protection) and be applied transversally, in a customized manner, depending on the domain of practice in the *social* spectrum (e.g., industrial sectors, smart environments). Additionally, regulations are complemented by good practices and guidelines developed to serve specific purposes (in this sense, ENISA has one of the most elaborate sets of guidelines for practical implementation of cybersecurity in different social areas, including Smart City).

Mapping of EU regulations on cybersecurity that impact Smart Cities



List of EU regulations on cybersecurity

1. Technical Cybersecurity

- [UN GGE on Developments in the field of information and telecommunications in the context of international security](#) (general principles for technological security)
- [EU Cybersecurity Strategy for the Digital Decade](#) (strategy for general cybersecurity)
- [Cybersecurity Act](#) (certification scheme & mandate for ENISA)
- [Regulation for ECCC](#) (technological sovereignty & financing & mandate for ECCC)
- [Proposal for Cybersecurity Regulation](#) (operational cybersecurity & mandate for CERT-EU)
- [NIS Directive](#) and [proposal for NIS 2 Directive](#) (directions for implementation of general cybersecurity measures)
- [Proposal for a Cyber Resilience Act](#) (security of products with digital elements)
- [Commission Recommendation on building a Joint Cyber Unit](#) (coordination of cyber operations)
- [Commission Recommendation on coordinated response to large-scale cybersecurity incidents and crisis](#)
- [Conclusions of the General Affairs Council on complementary efforts to enhance resilience and counter hybrid threats](#)
- [Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment](#)
- [Council Resolution on Encryption](#)

2. Complementary Cybersecurity

- [Charter of Fundamental Rights of the European Union](#)
- [EU Security Union Strategy](#) (strategy for extended, multi-domain security)

- [Regulation on restrictive measures against cyber-attacks](#) (incrimination of large-scale cyber-attacks)
- [Directive for incrimination of attacks against information systems](#) (incrimination of general cyber-attacks)
- [Proposal for a Regulation on cross-border preservation of e-evidence](#)
- [Council conclusion on Data retention for the purpose of fighting cybercrime](#)
- [Recovery and Resilience Facility](#) (financing)
- [Combating child abuse online](#)

3. Artificial Intelligence

(contains aspects related to security)

- [Artificial Intelligence for Europe](#) (which plays the role of an EU Strategy for AI)
- [White paper on Artificial Intelligence](#)
- [Proposal for an Artificial Intelligence Act](#)
- [Coordinated Plan on AI](#)
- [Ethics guidelines for trustworthy AI](#)
- [European Parliament resolution on AI in education, culture and audiovisual sector](#)

4. Disinformation

- [EU Action Plan against disinformation](#)
- [EU Code of Practice on disinformation](#)
- [EU Democracy Action Plan](#)

5. Digitalization

(contains aspects related to security)

- [The Digital Services Act package](#)
- [Digital Markets Act](#)
- [The European Digital Identity framework](#) and the proposal for Regulation eIDAS
- [Europe's Digital Decade: digital targets for 2030](#)
- [Digital Education Action Plan 2021-2027](#)
- [DigComp2.2 - The Digital Competence Framework for Citizens](#)

6. Data, and Data Protection

- [A European Strategy for Data](#)
- [General Data Protection Act](#)
- [Data Governance Act](#)
- [Directive on open data and the re-use of public sector information](#)
- [Directive on protection of natural persons with regard to the processing of personal data by competent authorities](#)
- [Directive on protection of natural persons with regard to the processing of personal data by the Union](#)

7. Critical infrastructures

- [Proposal for a Directive on resilience of critical infrastructure](#)
- [5G Cybersecurity](#)

8. Practical guidelines for Smart Cities

- [Council's conclusions on the Cybersecurity of connected devices](#)
- [ENISA's guide: Cyber Security for Smart City](#)
- [ENISA's guide: IoT and Smart Infrastructures](#)
- [ENISA Good practices for IoT and Smart Infrastructures tool](#)
- [ENISA's Cyber Security and Resilience of Intelligent Public Transport](#)

Cybersecurity Library



This section contains references to external materials related to Cybersecurity domain, with relevance for Smart City contexts.

The section is suited for:

- all audiences.

1. [Documentation related to Cybersecurity, with applicability to Smart City](#)
2. [Documentation related to social considerations of Cybersecurity](#)
3. [European institutions related to Cybersecurity](#)

1. Documentation related to Cybersecurity, with applicability to Smart City

Andrade, R.O., et al. (2020)	A Comprehensive Study of the IoT Cybersecurity in Smart Cities	A study exploring cybersecurity aspects and defining an assessment model of cybersecurity maturity of IoT solutions to develop smart city applications.
ENISA (2016)	Cyber Security for Smart Cities. An Architecture Model for Public Transport	An architectural guideline and good practices related to cyber security for public transport, in a Smart City context.
ENISA Online tool	IoT and Smart Infrastructures	A collection of good practices related to Cybersecurity of Smart Infrastructures, including Smart Cities.
Kalinin, M et. al. (2021)	Cybersecurity Risk Assessment in Smart City Infrastructures	An analysis of the methods for cybersecurity risk assessments in context of Smart City environments.
Ma, C. (2021)	Smart city and cyber-security; technologies used, leading challenges and future recommendations	A summary of good practices and architectural models for cybersecurity in Smart Cities.
MITRE ATTACK	Repository	A benchmark knowledge base of adversary tactics and techniques based on real-world observations, used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
NIST (2012)	Computer Security Incident Handling Guide. Special publication 800-61 Rev.2	A benchmark guideline related to cybersecurity incident management
NIST (2021)	Cyber-physical systems. NIST Smart Cities and Communities Framework Series	A collection of information on best practices in the field of smart cities and communities.
NIST (2022)	Glossary	A benchmark glossary with terms and concepts related to Cybersecurity.
New South Wales/ NSW	Cyber Security Policy	An Australian approach to cybersecurity policy that applies to Smart Places .
Popescu, E.F. (2021)	Dynamics of Cybersecurity. Landmarks for Holistic Management of Security in a Technological Context, 2nd Ed.	A book with conceptual and architectural overview of the Cybersecurity domain of science and practice, comprising both technical aspects and social considerations in relation to technology.
Pradhan, M. (2019)	Interoperability for Disaster Relief Operations in Smart City Environments	A framework and architecture model for ensuring technological interoperability in Smart City contexts, to handle disaster relief operations.
Vitunskaitė, M., et al. (2019)	Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership	A recommended framework encompassing technical standards, governance input, regulatory framework and compliance assurance to ensure all-layers security of the smart cities.

2. Documentation related to social considerations of Cybersecurity

Fuster, G.G., Jasmontaite, L. (2020)	Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights	An overview of the EU policies and legislative measures meant to regulate cybersecurity domain.
Papakonstantinou, V. (2022)	Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?	An analysis on the status, requirements and evolution of cybersecurity related laws and rights, at EU level.
EU practices related to Cybersecurity	Cybersecurity: how the EU tackles cyber threats	A summary of the EU practices to handle cyber resilience, fight cyber crime and boost cyber diplomacy and defence.
Markopoulou, D., Papakonstantinou, V. (2021)	The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular	An approach to define and protect critical infrastructures against cyber threats.

3. European institutions related to Cybersecurity

Cybersecurity Checklist for Smart Cities



This section contains a checklist with high-level actions to support the implementation of practical measures related to Cybersecurity of Smart Cities.

The section is suited, at least, for:

- SOC operators
- SOC supervisors
- Intelligence analysts
- Decision makers
- Policy makers
- Regulators

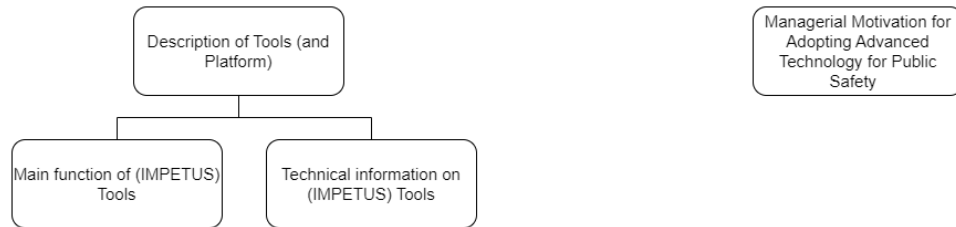


D6.2 - Cybersecu...ty Checklist.pdf

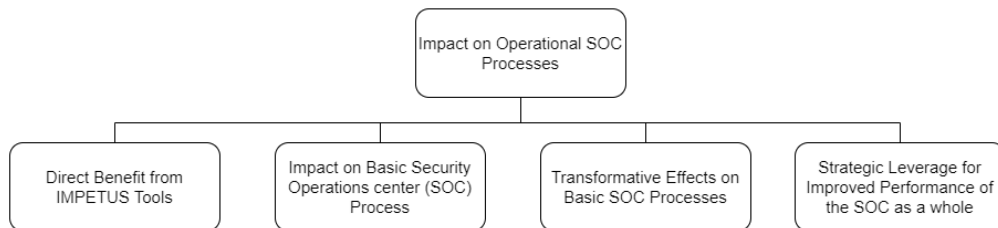
Practitioners Guide on Operations

Introduction and Readers Guide: Operations

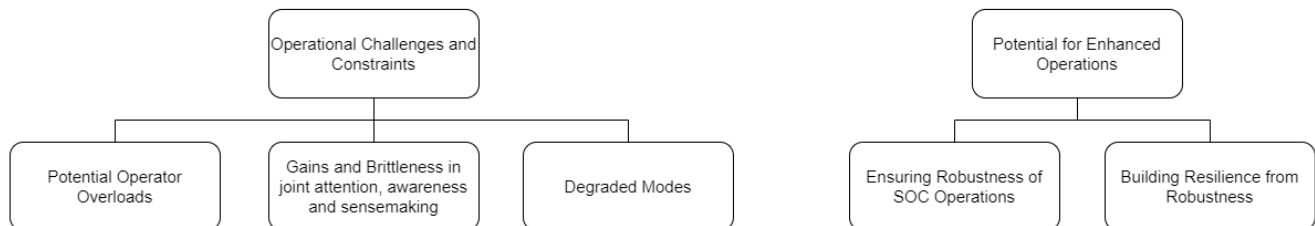
What is the IMPETUS platform and why would you want to use it?



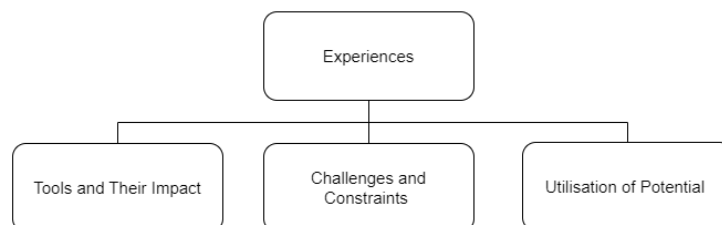
How to use IMPETUS in daily operations?



How can we enhance operational processes and handle unforeseen events with IMPETUS?



What are the operational experiences from IMPETUS deployments?



i This Practitioners Guide to Operations provides understanding and advice related to the nature, benefits, potentials and constraints of advanced IT tools used for public safety in the context of Security Operations Centers (SOC).

The **IMPETUS** solution is used as **an example** of measures applied to improve Operations in Smart City contexts, in order to illustrate how advanced IT tools can contribute to ensure a safe and reliable environment for the citizens and for the public administration. The PG presents the reader with a story that starts with an understanding of the tools in the IMPETUS solution, advances into a description of what impact they have for the SOC Operator and for the SOC operation as a whole for the benefit of public safety. It also makes the user aware of the key operational constraints and challenges of taking them into use, before it delineates the potential for long-term enhancement of SOC operation in terms of increased robustness and resilience capabilities.

For simplicity and recognition, the descriptions are focused on the SOC as a generic concept. Please have in mind that

- SOC's may be centralised or distributed. In the latter case, the individual SOC's may have specific purposes and profiles.
- Some useful IT tools may not have their primary use in the operational context of a SOC. E.g., for intelligence, social media analysis, workload monitoring of SOC operators, contingency planning (for instance for evacuation), or for gathering of training data for algorithms.

However, by use of modern network technology (here exemplified by the IMPETUS solution), these types of tools and their use may be seen as an extension of the SOC concept. E.g., various users will have the potential to participate in general awareness of operations in the SOC, maybe through a supervisor.

For a flexible reading experience, the root page and the various parts of the PG on OPERATIONS can be accessed and explored as desired.

The reading pattern illustrated below offers suggestions for specific audiences with presumed interests, to ease their orientation within the set of materials related to Operations and in correspondence with other subjects approached by the Practitioners Guides.

The recommended reading order is from top to bottom. This applies for each presumed readership (column)

As additional guidance, each suggested combination of content and audience is labelled either


E - Essential

I - Informative

IMPETUS Operations PG		Users of security solutions (current and prospective)						General Users	
		IT personnel	SOC Operator	Intelligence Operator	SOC Supervisor	SOC Security Manager	Innovation/OD manager, policy makers	Regulator/Official	General public /Citizen
Assumed interest of readership		Install, maintain and integrate tools in the IMPETUS solution	Utilize the tools in daily SOC tasks	Utilize the tools in background intelligence gathering for the SOC	Ensure that tools and solution are used coherently and effectively in daily SOC operations & collaboration	Assure that IMPETUS solution provides added value for public safety	Immediate impact and long-term, strategic advantage of the potentials in the IMPETUS solution and concept	Main benefits and operational challenges associated with the IMPETUS solution	Knowledge on what SOC's are doing for public safety
Main part of PG	Sub-sections								
Description of Tools (and Platform)	Main Functions of (IMPETUS) Tools	E	E	E	E	I	I	I	I
	Technical Information on (IMPETUS) Tools	E	I	I	I				
Impact on Operational SOC Processes	Direct Benefit from IMPETUS Tools	I	E	E	E	E	I	I	
	Impact on Basic Security Operations Center (SOC) Processes	I	E	E	E	E	E		I
	Transformative Effects on Basic SOC Processes	I	E	E	E	E	E	I	
	Strategic Leverage for Improved Performance of the SOC as a Whole	I	I	I	E	E	E	I	I
Operational Challenges and Constraints	Potential Operator Overloads		E	E	E	I			
	Gains and Brittleness in joint attention, awareness and Sensemaking		I	I	E	E	I		
	Degraded Modes		E	I	E	I			
Potentials for Enhanced Operation	Ensuring Robustness of SOC Operations	I	I	I	E	E	I	E	

	Building Resilience from Robustness				I	E	E	E	
Experiences	Tools and Their Impact		I		E	I			I
	Challenges and constraints		I		E	I	I	I	
	Utilisation of potentials				I	I	I	I	I

Description of Tools (and Platform)

 This section provides information about the main functions of the tools in the current IMPETUS solution from a user perspective, and links to technical information on each tool

This section includes the following subsections:

[Main Functions of \(IMPETUS\) Tools](#)


[Technical Information on \(IMPETUS\) tools](#)

The user-oriented tools are:

- Bacteria Detector - BD
- Cyber Threat Intelligence - CTI
- Cyber Threat Detection and Response - CTDR
- Workload Monitoring System - WMS
- Urban Anomaly Detector - UAD
- Evacuation Optimiser - EO
- Social Media Detection - SMD
- Firearm Detector - FD

The integration tool is:

- IMPETUS Platform

 Note that the term *IMPETUS platform* denotes a separate tool that centralises the outputs from the other tools in a single database and present them to the users.

Main Functions of (IMPETUS) Tools

A description of the complete package of tools of **The IMPETUS Solution, including the technical information of each tool**, is available [here](#).

Technical Information on (IMPETUS) tools

Bacteria Detector

Components of Bacteria Detector

BD combines two components: a bio-collector (developed by IMT/ UdN) and the Glow and Care which is the bacteria concentration measurement device. The first one acquires a sample of ambient air and catches the bacteria into water, the second one analyses this water to retrieve ambient air bacteria concentration.

Cyber Threat Intelligence

Components of Cyber Threat Intelligence

CTI has a few main components:

1. Manual Investigation - Deep dive into any escalation in real-time and understand the context.
2. Actionable Alerts - Pre-configured and automatically updated alerts and insights according to vertical and use case.
3. DVE Module - predicts the immediate risks of vulnerabilities with a higher probability of being exploited.
4. Case Management - Allows the user to track and manage an ongoing investigation by attaching pieces of information under a specific case, as well as sharing this information and progress with other colleagues.

Cyber Threat Detection and Response

Components of Cyber Threat Detection and Response

CTDR combines two components: Prelude and ELK Stack. Prelude-ELK is installed as a service on a Docker container, configured to receive syslog files from the components of the monitored system, using events messages on an IP network.

Workload Monitoring System

Components of Workload Monitoring System

The WMS tool provides its functionalities two-fold. On premises installation is for the **Server** component using a docker container and the delivery of pre-configures **Data Acquisition Units** (DAU's) to the end user.

Urban Anomaly Detector

Components of Urban Anomaly Detector

The UAD tool provides its functionalities "as-a-service". On premises installation is not available.

Evacuation Optimiser

Components of Evacuation Optimiser

The EO consists of an external tool for simulating evacuation scenarios. When provided, data from installed counter-person sensors can be used. No automatic systems/languages are currently provided to manage the flow of information (i.e. simulation of scenarios and analysis are performed manually by operators).

Social Media Detection

Components of Social Media Detection

The SMD tool provides its functionalities "as-a-service". On premises installation is not available.

Firearm Detector

Components of Firearm Detector

The tool is continuously deployed to monitor and look out for weapons in surveillance camera feeds, without any operator intervention.

IMPETUS Platform

Components of IMPETUS Platform

The IMPETUS Platform centralises the outputs from the tools in a single database and to present them to the users. The data is collected using two methods:

- API that is called by the platform (CTI)
- a message broker to which the tools push the data structured as JSON (all other tools)

The Platform also deals with the security aspects of communication with the tools and access to the data. The communication with the tools is done using an encrypted channel (using TLS). An authentication mechanism is implemented for tools and users access to the platform, followed by an authorization process – the tools are allowed to submit data only to certain topics from the message broker and the users are allowed to access the UI of the tools corresponding to their roles.

The platform consists of a set of docker images that contain the functionalities of the platform. The most important are:

- dashboard – contains the web application that implements the user interface of the platform
- dashboard-cron – contains jobs that run at regular intervals in order to prepare data that is presented in the user interface

- **iotapp-nr1** – contains a nodered instance used to create flows that get the data from the kafka message broker, transforms it and saves it in the database
- **kafka** – contains the message broker used to receive the data from the tools
- **dashboarddb** - contains the database used by the platform
- **ldap-server** – contains an openldap installation for managing the users and their roles in the platform
- **keycloak** – contains keycloak, an open source identity and access management solution, that is used to offer SSO capabilities for the components of the platform
- **rocketchat** – contains an installation of a messaging system
- **mongo** – contains the database used by rocketchat
- **wd-ui** – contains the user interface of the FD tool
- **wd** – contains the backend of the FD tool

Impact on Operational SOC Processes

i This section describes the fundamentals of the SOC processes.

In the subsections, direct benefits for SOC Operators from using IMPETUS tools, the direct impact from these benefits on the basic SOC work processes as conducted by SOC Operators, and the presumed leverage for improved performance of the SOC as a functional whole are described.

[Direct Benefit from IMPETUS Tools](#)

[Impact on Basic Security Operations Center \(SOC\) Processes](#)

[Leverage for Improved Performance of the SOC as a Whole](#)

Where the Impact Starts: The Basic SOC Operator Processes

The main context for application of IMPETUS tools and platform is the SOC processes, driven by SOC operators and enabled by technical and administrative support.

This operational context can be generalised into four primary processes:

- *Information collection* : retrieve relevant and correct information about the situation related to an incident or crises
- *Analysis* of information collected
- *Response activation* (possibly through an intermediary user operator at the scene of the crises)
- *Evaluation and correction* of response : feedback from as well as new input to the management of the incident or crisis

Direct Benefit from IMPETUS Tools

i This section describes direct benefit from IMEPTUS tools, along with a short description for context. A mote complete description of the tools can be found here: [Main Functions of \(IMPETUS\) Tools](#)

Bacteria Detector

Short description of BD
Continuously monitors air samples to detect abnormally high concentrations of airborne bacteria.
Benefits BD offers the opportunity to collect specific and reliable information about bacteria presence and concentration at locations of interest, including public spaces.

Cyber Threat Intelligence

Short description of CTI
Detects, classifies and helps mitigate cyberspace threats to an organisation's IT assets.
Benefits CTI offers the opportunity to receive information and be alerted about potential cyber attacks. Moreover, the tool offers to opportunity to analyse incidents, be offered guidance on vulnerable targets, and assess the effects of defensive actions.

Cyber Threat Detection and Response

Short description of CTDR
Detects cyber vulnerabilities in IT Systems: raises alerts and suggests countermeasures if they arise.
Benefits <ul style="list-style-type: none">• Users can scan complex systems to identify all vulnerabilities and their relationships• Users can monitor systems in real-time and receive an alert on the IMPETUS platform when a vulnerability has been exploited• Countermeasures can be prioritized based on the criticality of the threat

Workload Monitoring System

Short description of WMS
Measures mental workload and stress of emergency operators using a brain-computer interface, raises alerts if anomalies arise.
Benefits <p>This tool minimizes potential human error and improves human-machine teaming performance by monitoring the physical, emotional and mental workload status of operators while they perform their duties. It provides an early notification of an individual and/or a team's workload capability and ability to cope with stressors during emergencies.</p>

Urban Anomaly Detector

Short description of UAD
Continuously monitors data gathered from multiple city sensors and detects cases deviating from the norm - indicating possible cause for concern.
Benefits <p>The SOC operators will be able to better identify anomalous situations in crowd behaviour in public spaces.</p>

Evacuation Optimiser

Short description of EO
Provides instant advice to emergency staff on how to effectively manage an evacuation, based on simulations of different evacuation scenarios.
Benefits <p>Pre-optimises and supports the management of controlled crowd movement in public spaces in complex events, to prevent any injury and/or loss of life, e.g. in an emergency evacuation. Provides an accurate calculation of total evacuation time and risk to emergency operators.</p>

Social Media Detection

Short description of SMD
Scans large volumes of text on social media and other public online sites, looking for topics/keywords that might indicate potential trouble or threats.
Benefits <p>The SMD tool enables near online detection and alerts related to upcoming, unwanted events in the public spaces.</p>

Firearm Detector

Short description of FD

Continuously monitors surveillance camera feeds and automatically creates an alert if a firearm is detected in a public space.

Benefits

Improves the physical security of open spaces by reducing the response time to detect firearms, thereby reducing the risk of loss of life.

Impact on Basic Security Operations Center (SOC) Processes

The below description of impact builds on the description of the four primary SOC work processes as described [here](#).

Effectiveness and Efficiency of Basic SOC Processes

The effectiveness and efficiency of basic processes are influenced by a number of factors that may be supported and strengthened by the proper use of IMPETUS tools.

- Correct information that is quickly collected and accessible is essential for prompt response activation in SOC. Information may come from a variety of sources, such as cameras, human sensors, online sources or intelligence from collaborating agencies. Information that is unreliable or incorrect can introduce cascading consequences in operations as analysis and response are reactive to incoming information. Quite a few of the tools in the IMPETUS portfolio are reinforcing the information collection process in the SOC. E.g.,
 - The Bacteria Detector (BD) tool improves the SOC operation by introducing information about threats due to airborne bacteria in a timely and reliable manner
 - The Cyber Threat Intelligence (CTI) tool improves SOC intelligence activities by early identification of emerging threats and the "signatures" that will indicate their presence
 - The Cyber Threat Detection and Response (CTDR) tool enables identification of the initial stages of an attack graph of a presumed cyber threat, enabling online recognition of and selection of proper countering of an attack
 - The Urban Anomaly Detector (UAD) tool provides the SOC with early recognition of anomalous situations in public spaces
 - The Social Media Detection (SMD) tool provides the SOC with intelligence related to upcoming, unwanted events in the public spaces gathered from online sources.
 - The Firearm Detector (FA) tool enables real-time detection and alerts on the presence of firearms in public spaces
- Analysis of the information is vital in order to narrow down the volume of the information that is collected, to combine information coming from different source, and to retrieve the relevant information for the situation at hand. E.g.,
 - The Social Media Detection (SMD) tool has a set of filtering options for analysis which eases the process of finding the relevant information in a big dataset for the intelligence analyst/operator
 - The Cyber Threat Intelligence (CTI) tool provides advanced analysis filtering functions to find the relevant information about cyber related threats for a specific situation

Moreover, practically all IMPETUS tools contribute to a shared information picture that impacts the overall analysis process and enriches the grounds for shared situational awareness.

- Response activation to incidents may vary depending on the incident and information available, which levels are engaged, if there are several simultaneous incidents, situational awareness and other factors. The decision support provided can be vital to the operators' ability to succeed in their approach to incidents. E.g.,
 - The Cyber Threat Detection and Response (CTDR) tool enables tracking of an attack graph of an active threat, enabling the countering of the threat at many stages
 - The Workload Monitoring System (WMS) tool improves overall SOC operation by recognising fatigue and other stress impacts reducing the performance of SOC operators
 - The IMPETUS Platform enables joint access and effective coordination of relevant information among SOC operators
- A response can alter situations, not necessarily resolving them. For example, dispersing a group causing disorder may lead to scattering or relocation and not the end of the activity. If the response is not monitored and corrected the response may become insufficient or disproportionate. E.g.,
 - Practically all IMPETUS tools are able to update information continuously
 - The IMPETUS platform conveys all updated information, accessible for SOC operators

Transformative Effects on Basic SOC Processes

IMPETUS tools support, but also *changes the conditions* for the basic SOC work processes. Transformative effects are expected to materialize through experience and practical use, but some possible effects are possible to anticipate. For instance:

- CCTV-based surveillance creates a major (in practical terms unmanageable) attention problem where operators can only select a limited number of screens to monitor dozens or hundreds of cameras throughout the location of interest. As a result, CCTV-based surveillance can rarely allow detection in real-time and is most useful as a close to real-time or even forensics tool.
- **Tools Main Functions of (IMPETUS) Tools** like the **FD** have the potential to bring urban surveillance activity in (near) real-time for specific detectable events (e.g., presence of guns). This changes the nature of surveillance and role of the SOC in the direct management of these events.

- Tools like **SMD** or **CTI** raise similar issues of attentiveness related to intelligence operations: the increasing plethora of information to be considered makes it impossible to cover everything manually. This changes the nature of what it means to do intelligence analysis. However, it does not remove the analytical part the intelligence operators are responsible for.
- **UAD** can give early indications but also potentially let the operator track the consequences of response triggered by other tools, and cascading consequences
- **BD** as an entirely new capability affects both detection and response; e.g., in the case that it gives an alert during an evacuation
- **EO** can be used to plan for different alternatives, and thus enable a more adapted and dynamic evacuation that responds to new information, for instance from UAD, during evacuation.
- **CTDR** propose countermeasures based on detection, while **WMS** monitoring might impact the actual capability to act, e.g. by recommending changed tasking of operators

A common platform (e.g., IMPETUS) allows for exchanges of information between security actors who currently do not have ways to coordinate directly, for instance between intelligence actors and SOC operators. This capability has the potential to support a shift towards a more unified response to events, emancipating from siloed handling of urban security.

Similarly, transfers of data are available by simple “clicks”, allowing for instance field operators and SOC to exchange images rapidly and purposefully.

The changes in information pathways and utilisation from using the platform inside one single actor (e.g., a SOC) creates the opportunity and ability to synthesise types of information that previously were not neither conceivable nor available. This will affect both operations, and the operators' competence.

Strategic Leverage for Improved Performance of the SOC as a Whole

i In this section, we address perspectives and possible actions for strategically leveraging improved capabilities and performance of the SOC as a holistic entity, enabling interaction with other entities and actors engaged in incident and crisis management in public spaces.

As described in [Transformative Effects on Basic SOC Processes](#), it might be expected that SOC processes are transformed in an emergent way, driven by practice and experience.

In addition to, but not hindering experience-based transformation, improved performance can also be leveraged in a more strategic manner. The strategic goals may for instance be to enhance a SOC's interaction with other active agents physically closer to and in direct intervention with the event, and/or to enhance collaboration between a diversity of SOC's.

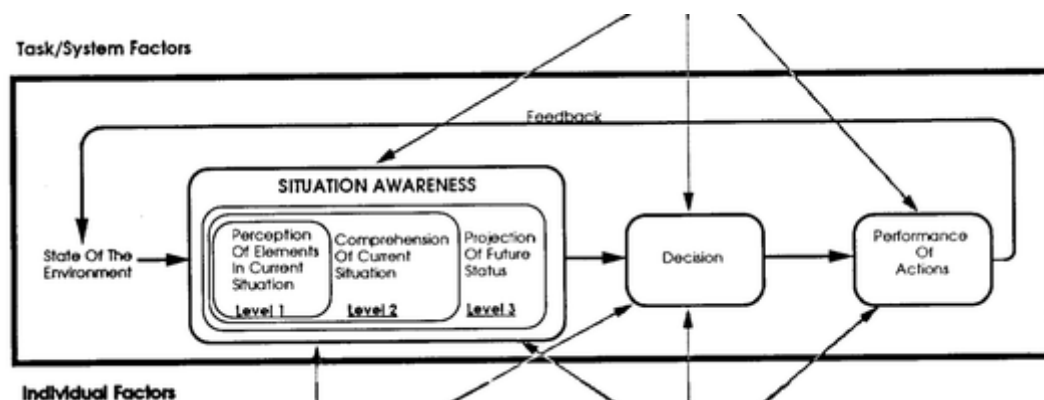
To frame such a strategic leverage, we will here present

- a strategic **perspective**, that enables
- a number of **strategic foci** for leverage of enhanced operation within, between and together with SOC's

Strategic perspective for leverage

The term **situational awareness** (SA) is pivotal to understanding the overall impact on the SOC processes. [\[Endsley 1995\]](#) defines situation awareness as “the **perception** of elements in the environment within a volume of time and space, the **comprehension** of their meaning, and the **projection** of their status in the near future”.

This is consistent with the four basic SOC processes; information collection, analysis, response activation, evaluation and correction, and their interactive nature.



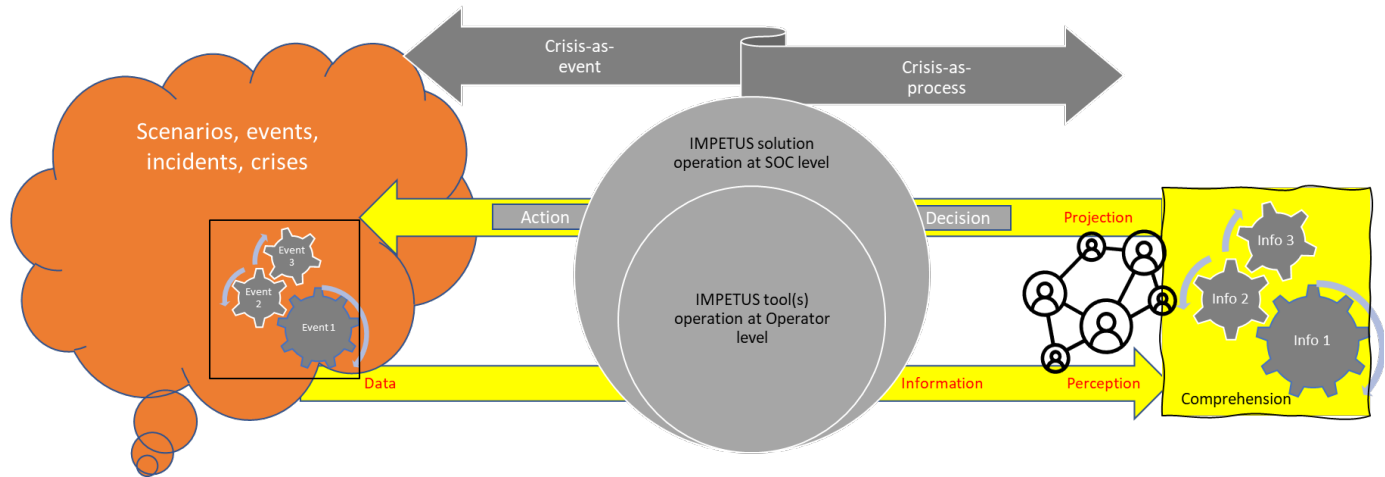
For our purpose, we need to adapt these concepts to the IMPETUS context in order to describe the potential additional leverage from the IMPETUS solution. This is done by distinguishing between the *crisis-as-event*, and the *crisis-as-process* (in and between the SOC environments and other collaborators), with the IMPETUS solution as an intermediary, as illustrated in the figure below.

The motivation for this is twofold:

- To persistently keep in mind the distinction between the real events, and the way they are re-presented by digital tools. Re-presentations are most often useful and sufficient, but never exact, and not seldom poorly contextualized.

- To be aware that the way people collaborate to cope with an event - the crises-as-*process* - might break down by itself, independent on how the crises plays out in the real world. In case, with potentially fatal consequences for the management of the crises-as-event

By employing this perspective, we will be able to both harvest the advantages from advanced IT tools, without running the implicit risk of fatal breakdown in the collaborative patterns.



Strategic foci for leverage

Here, we identify a selection of strategic foci which enable proper reasoning about potential strategic leverage:

- Reinforced appreciation of the Operators' role
- Joint understanding and awareness
- Improved access to data for decision-making used as reinforcement of existing capacities
- Rebalancing SOC-structure and operational patterns to utilise new information pathways
- Changes in communication patterns: common operating language

The IMPETUS solution and associated tools will be used as illustrative examples.

Reinforced Appreciation of the Operators' Role

Maintained appreciation of operators' role in current-day operations is crucial for leveraging the full impact of the IMPETUS solution. While it may be tempting to downplay the operators' role when introducing powerful technologies, the very opposite attitude should prevail: how can the tools support and enhance the operators' role?

Operators convey context-appropriate information that can be cascaded to all levels of an organisation to support rapid decision-making. Analytical reasoning provides the foundation for the abstraction of data at multiple levels to convey the right information at the right time and place. The goal of the analytical reasoning is to make a judgement about an issue. Operators often form their judgements under significant time pressure and with limited and conflicting information. Their judgements reflect their best possible understanding of a situation, including assumptions, supporting evidence, and uncertainties.

The challenges associated with this are so complex and dynamic that they cannot be addressed by individuals working in isolation. Hence, operator scalability plays an important role. Systems such as the IMPETUS solution must support the communication needs of these groups of operators working together across space and time, in high-stress and time-sensitive environments, to make critical decisions. Collaboration may be broadly defined as the interaction among two or more individuals and can encompass a variety of behaviours, including communication, information sharing, coordination, problem solving, and negotiation.

Joint Understanding and Awareness

Situational awareness (SA) comprises individual operator's understanding of what is going on, but is also an aggregate of individual understandings working together. From a crisis management process effectiveness and efficiency standpoint, a harmonised or *aligned* SA may seem preferable. Such a preference may however overshadow an important issue; is the aligned SA fit for purpose?

The term *brittleness* addresses a sudden collapse or failure when events push a process up to and beyond its boundaries for handling changing disturbances and variations. Brittleness is therefore a condition that may cause that something apparently stable turns out to be *fragile*. An overly aligned joint SA might turn out to be fragile if the inherent brittleness is not noticed nor addressed.

We therefore distinguish between the *joint* and the *aligned* SA: The latter may *appear* functional but may be brittle and turn dysfunctional (fragile) because it lacks the ability to recognise and adjust to small but important deviations in and weak signals from the crises-as-event. A more functional *joint* SA facilitates swift collaboration but do not suppress individual deviation that might be instrumental for making sense of and raising joint awareness from small deviations in and weak signals from the crisis-as-event.

To avoid brittleness, a joint SA must not become static. In practice, a joint SA is always a matter of negotiation and compromise, and diversity of individual SAs can therefore also be a source for a more dynamic, adaptable, and functional joint SA in complex environments. This requires a

continuous trade-off between effectiveness and efficiency under time constraints, and between diversity and alignment. These trade-offs will be mostly visible in the context of primary SOC operator processes 3 and 4 (activation and correction).

The IMPETUS solution conveys the potential of improving both individual and joint SA, by providing more information and assistance in decision support. By training and careful development of clear and concise but flexible procedures before and while the IMPETUS solution is incorporated in daily operations, both individual awareness and joint "awareness about awareness-as-process" can be raised. This is an important reason why IMPETUS provides a "green field" for SOC operations, which may be formative and instrumental for the persistent enhancement of SOC operations in complex situations.

Improved Access to Data for Decision-making Used as Reinforcement of Existing Capacities

The IMPETUS solution will contribute with data from many different sources which extends the SOC information space substantially. Moreover, several of these tools employ Artificial Intelligence (AI) for collecting and analysing information. Hence, IMPETUS will convey an increase in both the quality, relevance, and volume of information.

This increase may however have an overwhelming effect on the user/operator. A number of issues are important for IMPETUS solutions having a positive effect on SOC performance, namely

- Manning assessment, including number of tools per user, and division of responsibilities clarified based on authority and set of skills.
- Appropriate training calibrated to different end users, promoting understanding on how to efficiently use the different tools and how to analyse and understand the platform output, including awareness of limitations and shortcomings of the technology, and the need for human-in-the-loop.
- Clarifications of responsibilities and mandates for correlating and combining the platform output and making decisions based on the findings.
- Awareness of biases in AI tools, and proper organising of human monitoring before decisions/actions are taken based on AI output

That is, given that the established experience and skills of various SOC operators is acknowledged and appreciated as the point of departure, the thorough assessments, and deliberations on the use of the IMPETUS tools will likely reinforce the existing individual capabilities of the SOC operators, and enhance their collaborative capability. While a potential fragility will persistently be embedded in these complex interactions, an important type of insurance will be to ensure that the benefits from practices of using the tools do not erode the operators' deep theoretical or functional understanding of the underlying systems, and the arenas to which decisions and advice are forwarded. This will also be a necessary "premium" for IMPETUS becoming formative for long-term enhancement of resilience of operations in complex situations.

Rebalancing SOC-structure and Operational Patterns to Utilise New Information Pathways

To maintain momentum on the potential improvement from the IMPETUS solution, it may be necessary to redefine the chain of command, information flows and decision patterns.

This will require that key aspects such as information pathways and SOC-structure must be realigned and re-balanced. The added information access from the platform and the new operator role may lead to a different information sharing pattern. This can apply to information sharing between the SOC-operators themselves, as well as sharing with SOC-supervisors, decision makers and external first responders. One can also envision a change to the number of SOCs and the number of operators in the different SOCs. For instance, the IMPETUS solution could be viewed as a digital co-location of SOCs resulting in the need for fewer SOCs.

Due to these changes, it may be necessary to define the chain of command for personnel that are working with the IMPETUS solution. Who is informing who about the findings from the tools? Who makes decisions based on the information? Roles, tasks, and responsibilities in the decision-making process should be defined clearly in the new concepts of operation. It will be necessary to develop training and Standard Operating Procedures (SOPs) to address these changes and formalise the new baselines. Baselines will however always be challenged and must therefore also be robust. The principles for strengthening interaction in distributed organisations are for instance pivotal to the Crew Resource Management (CRM) training procedures.

Changes in Communication Patterns: Common Operating Language

Information flows are implemented through interactive communication patterns and protocols incorporating humans, and will consequently also need to be changed to accommodate changes in information flows. This requires a sociotechnical approach.

Using the IMPETUS solution, it is likely that involvement of personnel across different organisations will change existing communication patterns within the organisations involved. A common terminology and symbology is needed when communicating about platform findings, inputs, outputs, work, and response processes. It is important to consider that both operational SOC personnel and external first responders may be using other platforms and systems that might have different terminology and symbology. Moreover, they might already have their own procedures and protocols for communication during emergency response.

These factors must be considered when making the training programs for the platform. Developing a systematic overview of information elements that are critical to share in different crisis scenarios and striving for terminology harmonisation can help ensure interoperability. However, existing communication processes and practises must be also considered.

Despite that this task may appear merely as a price to be paid, it is also an opportunity to mutually sensitise different users to each other's operational outlook and key aspects. Such mutual sensitivity will be very valuable for the "awareness of awareness" negotiations needed to avoid joint forgetfulness, potentially compromising the joint SA.

Operational Challenges and Constraints

i In this section, we address operational challenges and constraints related to different types of overload, brittleness in joint attention, awareness and making sense of situations, and a number of foreseeable degradations of the IMPETUS solution. These are each described in the separate pages which follow:

Potential Operator Overloads

Gains and Brittleness in Joint Attention, Awareness and Sensemaking

Degraded Modes

Potential Operator Overloads

i SOC Operator overload and saturation may jeopardise the potential gains from the IMPETUS solution. The precautionary means can be aligned with the enabling means.

The IMPETUS solution will contribute with data from many different sources which extends the SOC information space substantially. Moreover, several of these tools employ Artificial Intelligence (AI) for collecting and analysing information. Hence, IMPETUS will convey an increase in both the quality, relevance, and volume of information. This increase may however have an overwhelming effect on the SOC operator.

Data/information overload may be seen as "a condition where a domain practitioner, supported by artifacts and other human agents, finds it extremely challenging to focus in on, assemble, and synthesise 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" [Woods et al., 2001]. This is an imminent danger for practically all users of IMPETUS tools, not at least because IMPETUS users might also be responsible for monitoring other sources, in addition to the IMPETUS platform. To avoid that the operators will struggle with data overload or work overload related to task management, several organisational issues should be raised in conjunction with the introduction of IMPETUS tools. The same issues that are highlighted for reaping the benefits from the IMPETUS solutions, will also be occasions for defining precautionary means against overload and saturation of SOC operators, namely:

- Manning assessment, including number of tools per user, and division of responsibilities clarified based on authority and set of skills.
- Appropriate training calibrated to different end users, promoting understanding on how to efficiently use the different tools and how to analyse and understand the platform output, including awareness of limitations and shortcomings of the technology, and the need for human-in-the-loop.
- Clarifications of responsibilities and mandates for correlating and combining the platform output and making decisions based on the findings.
- Awareness of biases in AI tools, and proper organising of human monitoring before decisions/actions are taken based on AI output.

Gains and Brittleness in Joint Attention, Awareness and Sensemaking

i In this section, we contrast the potential gains with the potential brittleness emerging from using IMPETUS tools. The key themes are attention to events, awareness of situations and developments, and the crucial process of making sense of these for making the right decisions and choosing the proper actions.

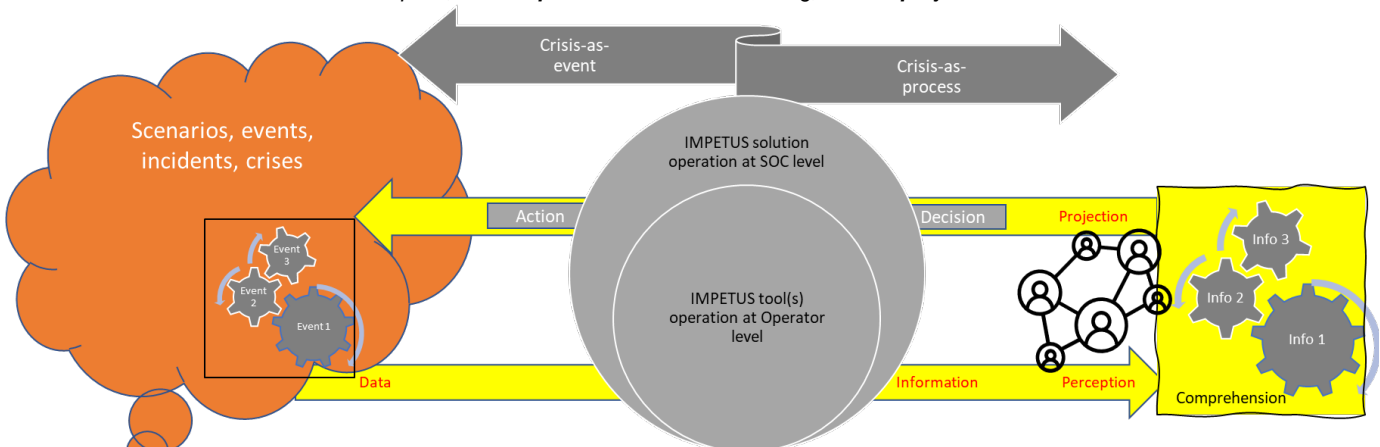
Connecting Attention, Awareness and Sensemaking

These concepts are connected to a vast scientific literature that we here attempt to simplify for the making of a few key points.

The IMPETUS solution provides information to the SOC and other from data collected from the real events. In our perspective, this implies a distinction between the *crises-as-event* and the *crises-as-process*, in which the IMPETUS solution is an intermediary.

At a very basic level, the *crises-as-process* is a about *attention*, the operators' ability to attend to the information space without suffering overload or congestion.

The next issue is the broadly used term situational awareness. [Endsley 1995] defines *situation awareness* as "the **perception** of elements in the environment within a volume of time and space, the **comprehension** of their meaning, and the **projection** of their status in the near future."





In our *crises-as-process* SOC context, the perception is very much based on information based on data from IT tools. This applies for the individual SOC operator, rendering the possibility open that different operators may *perceive* differently, as well as *comprehend* and *project* differently, if they are not properly coordinated.

Sensemaking is a perspective that highlights that perception, comprehension and projection are not neither linearly nor unidirectional connected. Sensemaking is not a deterministic, but a complex process influenced by cues and overarching search for meaning and comprehension. While we habitually think that what we see is what we believe, sensemaking ultimately implies that “what we believe is what we see”. This is urgent to keep in mind when a complex and surprising *crises-as-event* is comprehended in the *crises-as-process*, involving a diversity of operators under strain. In extreme uncertainty, what is believed (to be seen) might have to be instantly *created* out of very few cues.

The brittleness of joint understanding and awareness

Situational awareness (SA) thus comprises individual operator's understanding of what is going on, but is also an aggregate of individual understandings working together. A diversity of individual SAs can be a source for a more dynamic, adaptable, and functional joint SA in dealing with complex situations. In practice, any degree of **joint SA** is always a matter of negotiation and compromise, and the result of this may have different implications.

Any individual SA can be influenced by errors, such as failing to understand critical signals relating to a process being monitored, inadequate interpretation of information, insufficient understanding of responsibilities, and inadequate communication within teams [Johnsen et al. 2020]. Within the aviation sector, it has been observed that use of technology and automation leads to reduced situational awareness [Endsley 1996, Endsley 2015]. This is linked to the fact that humans who are monitoring work processes where they are not actively involved (out-of-the-loop) may become less attentive.

Upholding a functional joint SA is therefore a big issue, entangled in tiny differences that may escape attention. If oral, written or other communicative acts and deliberations needed to negotiate and align individual SAs are neglected or overrun, a joint forgetfulness and ignorance of important anomalies, weak signals and warnings may lead to an aligned, but dysfunctional joint SA.

The IMPETUS solution conveys the potential of improving both individual and joint SA, by providing more information and assistance in decision support. However, end users need to be aware of the risks pertaining to operators becoming “out-of-the-loop”, potential failure to maintain attention levels, and the potential joint ignorance and forgetfulness driven by ignoring the small things of communication. The new and extended information space and information pathways might also affect the negotiations of (joint) awareness in dysfunctional manners. e.g., when instant supply of new and fresh information may appear to provide or offer instant understanding that fill information voids or justifies default operational actions.

It is therefore necessary to acknowledge the crucial role of the apparently “redundant” work necessary to unite and reconcile incompatible assumptions and procedures. This raises a challenge, as this type of work is characterised by the fact that it apparently solves inconsistencies by packing up compromises that “get the job done”, which solves the situation locally and temporarily so that one can move on. Such “closure” is about creating unity, but this unity can also be about ignoring something crucial just because it is hard to resolve [Grøtan, 2020].

Degraded Modes

i In this section, impacts from degradation of the IMPETUS solution are identified, along with the recommended action to prepare.

Note that this not include cyber-security issues, as these are the subject of a separate Practitioners Guide.

The IMPETUS solution comprises a number of independent tools, and an IMPETUS solution that integrates them in a common interface.

Malfunction of Tools

In case of malfunction of a specific tool, two outcomes are possible

- the malfunction of the tool affects the primary SOC work processes in a limited sense
- the malfunction has a severe impact on operation of the SOC as whole, e.g., the additional gain on situational awareness (see [Strategic Leverage for Improved Performance of the SOC as a Whole](#))

For the latter case, specific scenarios of tool malfunction should be integrated as part of the preparation for Robustness and Resilience (see Section: [Potentials for Enhanced Operation](#)).

In these scenarios, the impact for the SOC Operator and for the IT Personnel should be seen as separate cases.

Malfunction of the IMPETUS Platform

In case of malfunction of the IMPETUS platform, two outcomes are possible:

- Some tools may be able to operate separately
- Some tools may not be accessible

Based on an updated oversight of the characteristics of each tool in case of platform malfunction, specific scenarios of platform malfunction should be integrated as part of the preparation for Robustness and Resilience (see Section: [Potentials for Enhanced Operation](#)).

Potentials for Enhanced Operation

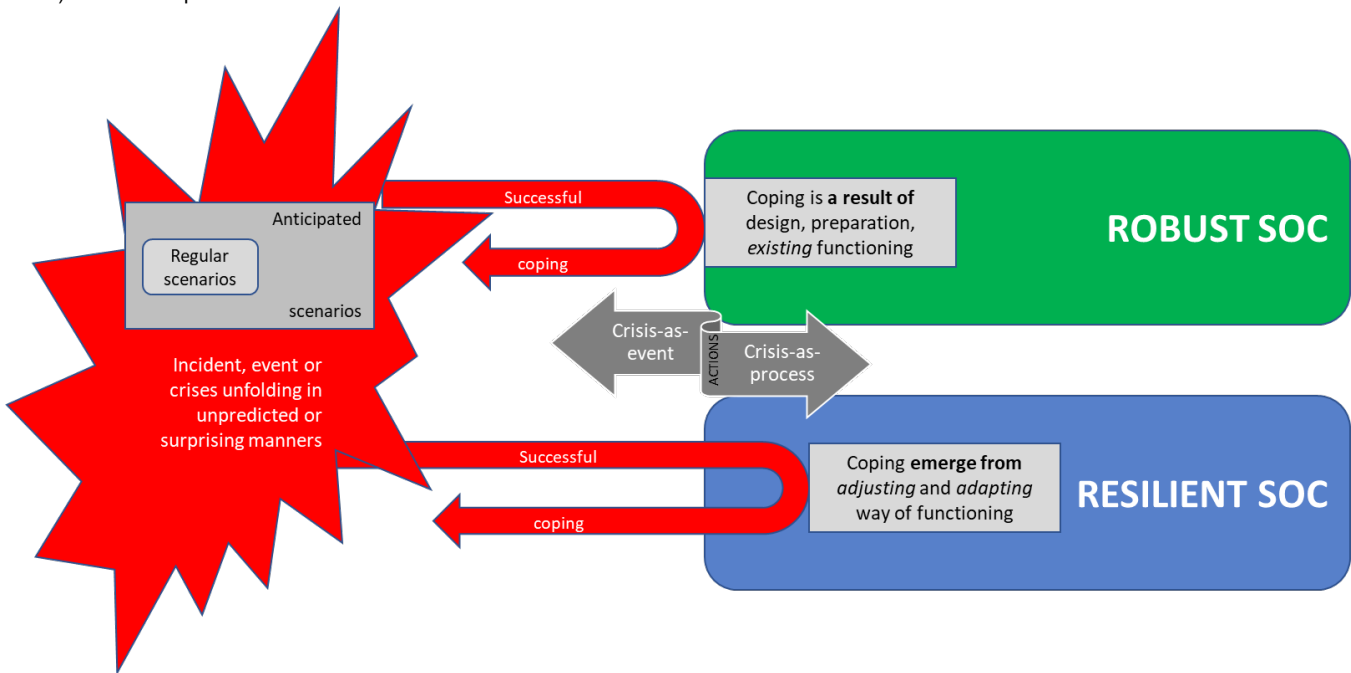
i Security Operations Centers (SOC) must be ready to deal with a wide diversity of incidents, events and crises, spanning from the trivial to the unprecedented and genuinely surprising. Their operational agility - the ability to withstand and cope with unpredictable and surprising situations - requires both Robustness and Resilience. Robustness is necessary but not always sufficient. Resilience is the complementary approach in which adaptive capacities are built to prepare for the unexpected.

This section includes the following subsections:

[Ensuring Robustness of SOC Operations](#)

[Building Resilience from Robustness](#)

Regardless of well the crises management processes are transformed through experience [Transformative Effects on Basic SOC Processes](#) or improved through strategic leverage [Strategic Leverage for Improved Performance of the SOC as a Whole](#), specific and sustained attention should be paid to the operational **robustness** and **resilience**, to avoid that the crisis management process (“**crisis-as-process**” in the figure below) fails or collapses.



Robustness and Resilience - a crucial distinction

A **Robust** SOC is able to successfully cope with the unexpected as a result of being planned, designed or implemented to absorb perturbations beyond what is anticipated.

A **Resilient** SOC is able to successfully cope with the unexpected in an emergent way by being able to adjust and adapt its way of functioning in “real time”, in an effective manner related to how the unexpected situation actually arrives and presents itself.

SOCs will benefit from building **both** Robustness and Resilience. In this section we will sketch out how the IMPETUS solution may be utilised in a process of building such capabilities.

Event vs. (SOC) Process

Both perspectives will benefit from a distinction between: (see also [Strategic Leverage for Improved Performance of the SOC as a Whole](#))

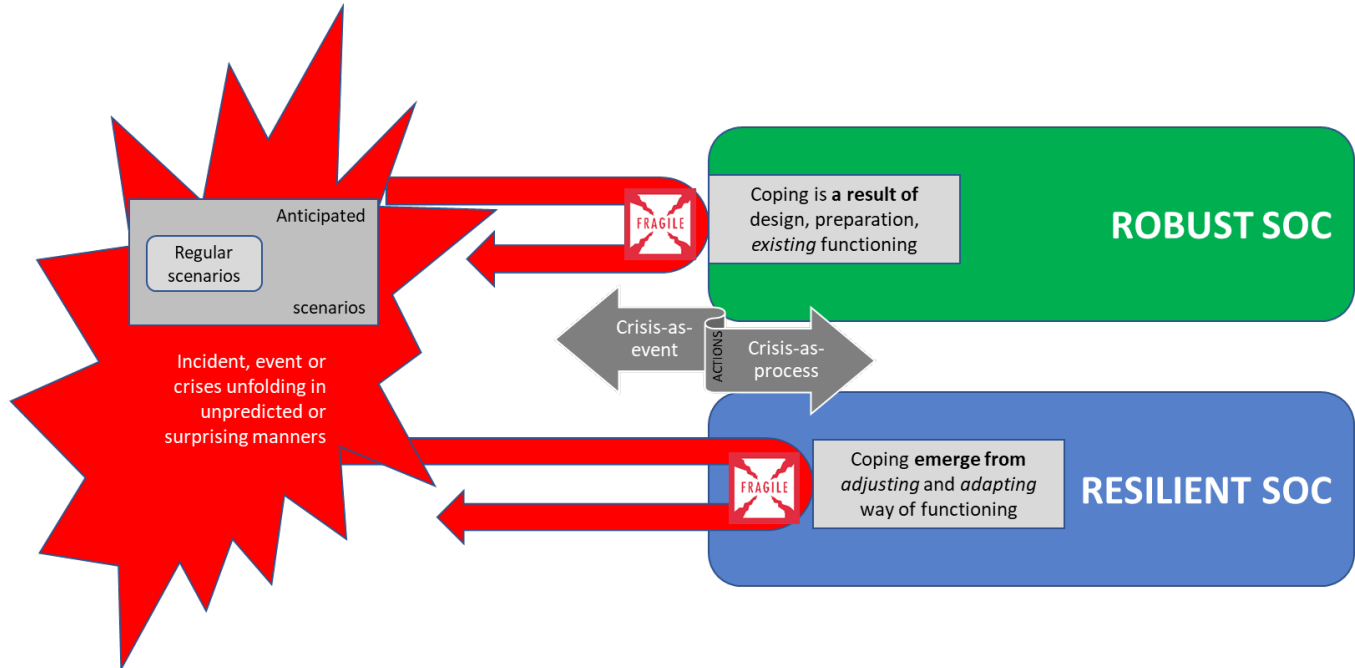
- The *crisis-as-event*: the events (in public spaces) and the dynamics between them, including the influence from the actions taken by the SOC
- The *crises-as-process*: the (SOC) working processes that produces the actions taken by the SOC

This distinction is based on the broad conceptualisation by [\[Williams et al., 2017\]](#), but here we use it for a specific purpose, namely to highlight the potential enhancement of SOC operations by means of the capacities of IMPETUS tools, as well the potential brittleness and fragility embedded in this potential.

Two Interrelated Types of Brittleness and Fragility

Neither Robustness nor Resilience can guarantee success.

The term *brittleness* addresses a sudden collapse or failure when events push a process up to and beyond its boundaries for handling changing disturbances and variations. Brittleness is therefore a condition that may cause that something apparently stable turns out to be *fragile*.



- Robustness may therefore be brittle at the boundaries of preparedness; when perturbations and the dynamics of the events overwhelms existing functionality. Fragility of Robustness as a capability is therefore mainly visible related to *crisis-as-event*.
- Resilience may be brittle when the (inevitable) limits and boundaries of adaptive capacities are encountered. Fragility of Resilience as a capability is therefore mainly related to *crisis-as-process*.

The two types of brittleness and fragility are thus different, but interrelated. Robustness may also be brittle due to improper implementation. At the other extreme, if Robustness is the dominant approach, attempting to prepare for “any” scenario, it may jeopardise adaptive capacity (constituting resilience). Scholars like [Woods 2019] argue that such systems may be “robust, yet fragile”. This pertains especially to *crises-as-process*.

Keeping Woods' (2019) warning in mind [Woods 2019], it is nevertheless recommended to build Robustness as a foundation. The actual balance point between Robustness and Resilience must be found by each unique organisation. The good news is that the IMPETUS solution may be a platform for capacity building for both Robustness and Resilience of the *crises-as-process*.

The IMPETUS Tools and Solution as a Base for Capability Building.

Neither Robustness nor Resilience capabilities comes for free, both have their inherent limits, but they can be gradually built through a deliberate process, in which an IMPETUS type of solution is at centre stage.

The IMPETUS solution may be seen as an intermediary; the “eye” observing the *crisis-as-event* as influenced by SOC decisions and actions, and a collaboration arena for the *crises-as-process*. In understanding the potential influence of IMPETUS solution as an enabler for capability building, we distinguish between:

- The influence on each SOC operator's contribution to working processes (as described in *Impact on Operational processes>Impact on basic SOC processes*)
- The influence on the SOC working processes as a whole (as described in *Impact on Operational processes>Leverage for improved performance of the SOC as a whole*)

The initial preparation for the capability building will be that the actual SOC/organisation outlines its own interpretation of the above impacts. That is, an assessment on how the actual portfolio of tools will impact each SOC Operator's contribution to the work processes, and how this can be leveraged into a higher performance with respect to, e.g., joint situational awareness for the SOC operation.

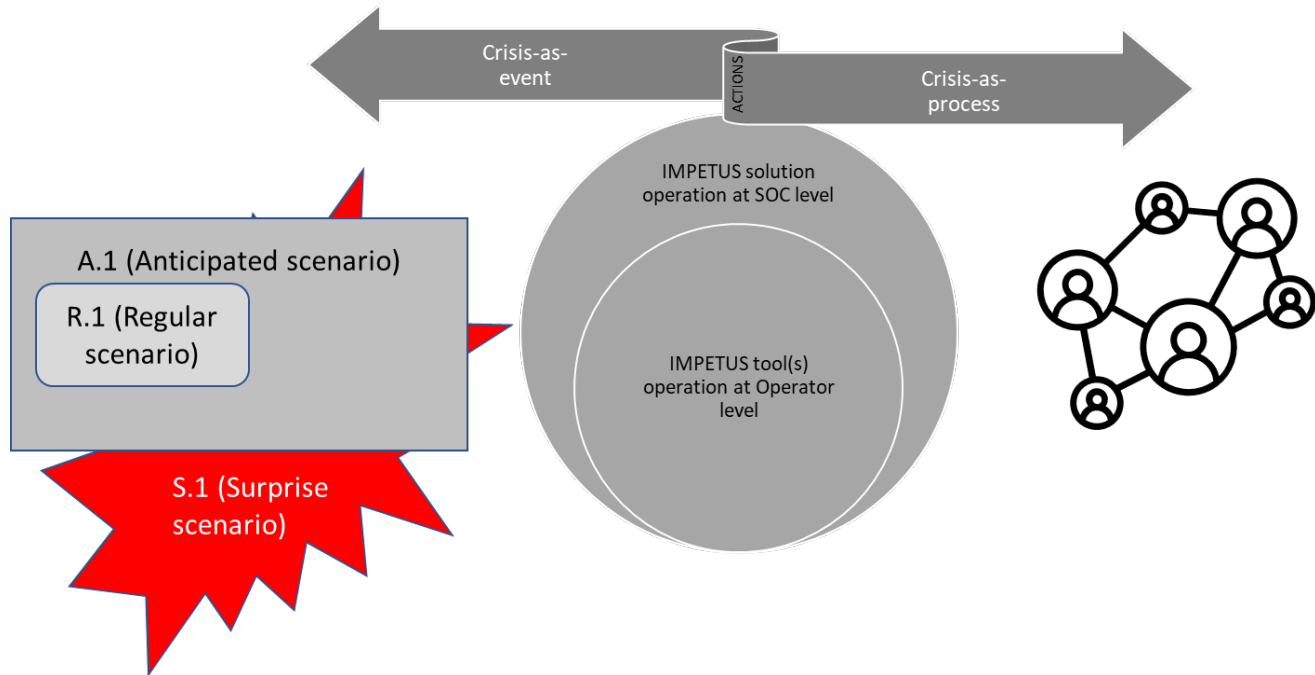
Scenario Preparation

Moreover, capability building of Robustness and Resilience will require that three types of scenarios of the *crises-as-event* are outlined from the start.

1. A **Regular** scenario which the actual SOC and Operators are very familiar with
2. An **Anticipated** scenario reflecting an “irregular”, anticipated scenario and set of events which the SOC and Operators, however, are confident they will be able to identify the proper actions towards
3. A **Surprise** scenario partly building on the Anticipated scenario, but which is escalated in a manner which is considered unlikely but not impossible, and in which proper actions and responses are not yet identified

They are labelled **R.x**, **A.x** and **S.x**, respectively, to signify that will need to be updated regularly to support a progression in the development of robustness and resilience.

These three scenario types will be the point of departure for capability building in the crises-as-process domain, with the IMPETUS (type of) solution as an intermediary for both the SOC operator and the SOC as a whole.



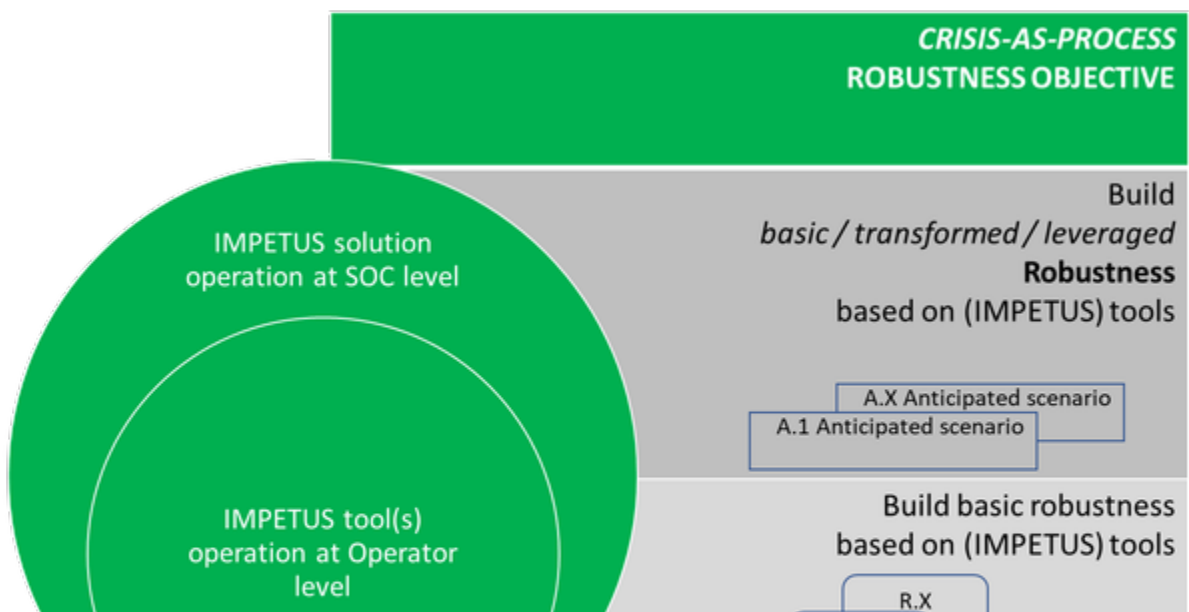
In the following, a stepwise approach for building Robustness and Resilience capabilities, respectively, will be outlined in separate sections. However, especially as Resilience building is a never-ending story, it is important to start from the right angle. That is, Robustness is a comparatively more stable property that can be *built* and thereafter *ensured*, while Resilience is the more fragile property that must be continuously *built and renewed*.

- [Ensuring Robustness of SOC Operations](#)
- [Building Resilience from Robustness](#)

Ensuring Robustness of SOC Operations

i In this section, we outline how Robustness can be established and ensured through recurring validation, stress-testing and revising.

BUILD Robustness

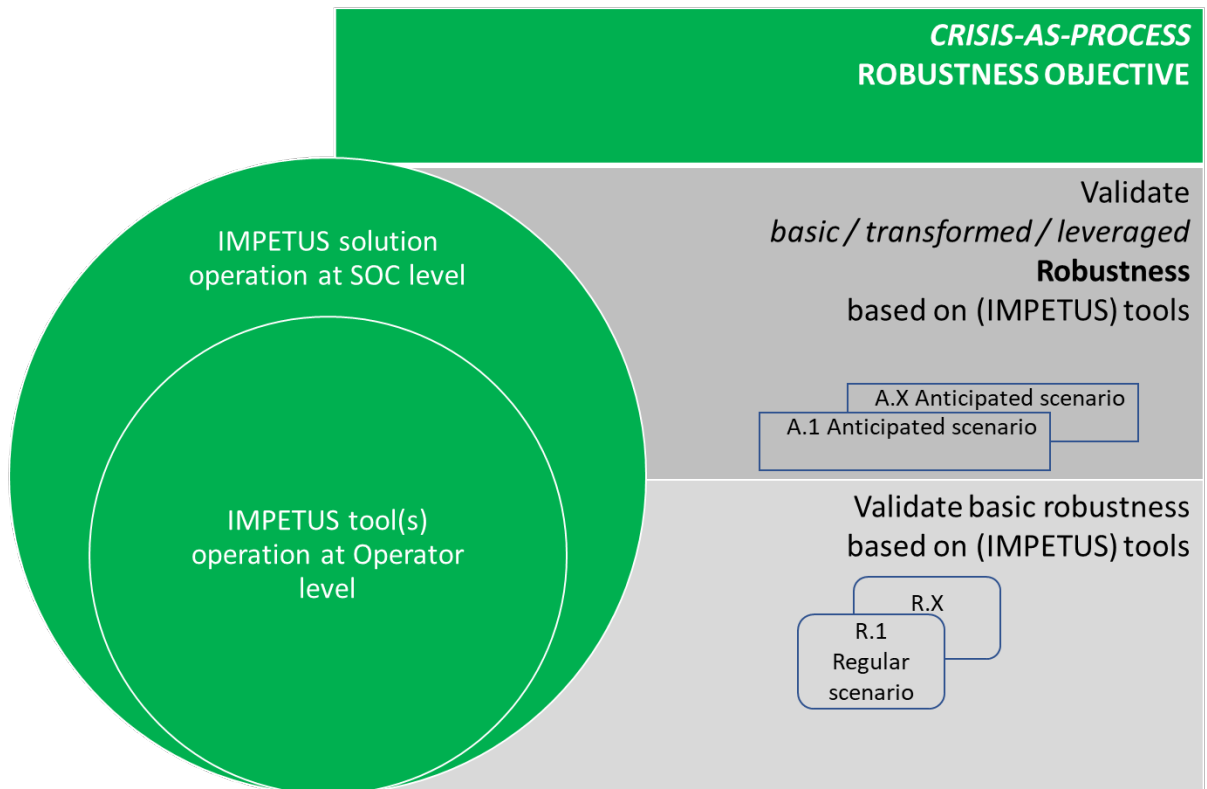




Based on the Regular scenario, procedures for the SOC Operator are defined.

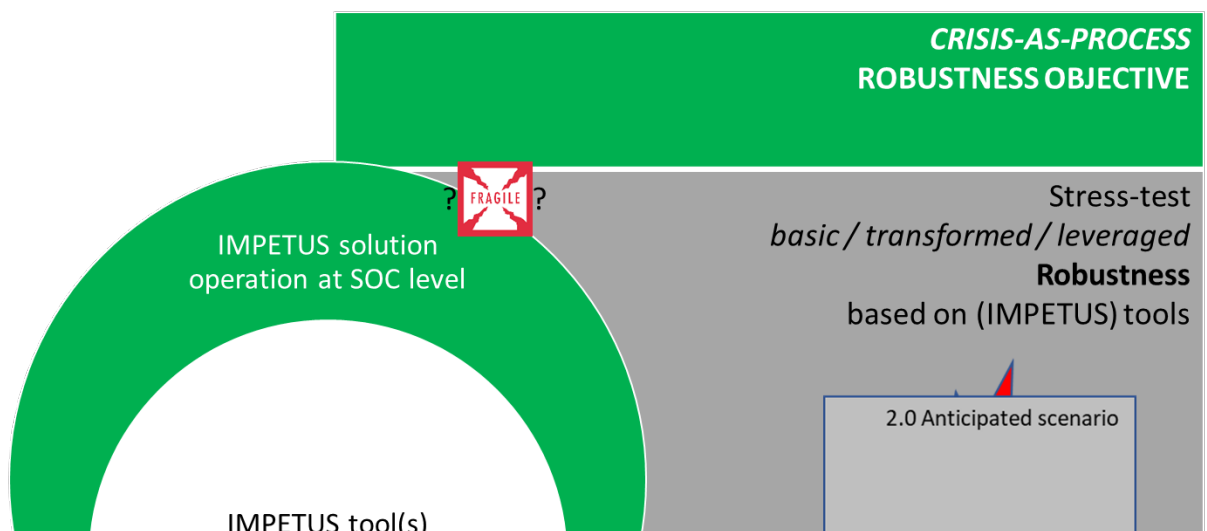
Based on the Anticipated scenario, plans are developed for how each Operator will contribute, and the benefit from each tool is anticipated, in a manner that reflect the maturity of the organisation related to the anticipated potential for **transformation** ([Transformative Effects on Basic SOC Processes](#)) or **strategic leverage** of SOC performance ([Strategic Leverage for Improved Performance of the SOC as a Whole](#)).

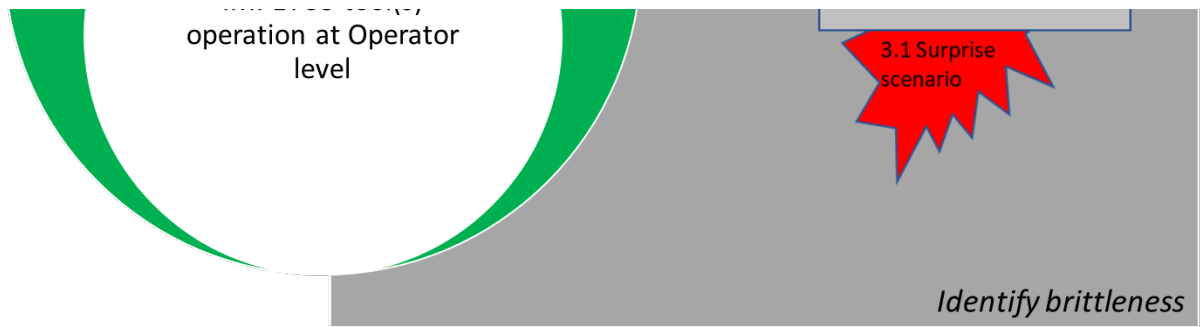
VALIDATE Robustness



The SOC should recurrently validate that Robustness is maintained. Revisions of the Regular and Anticipated scenarios should be done periodically.

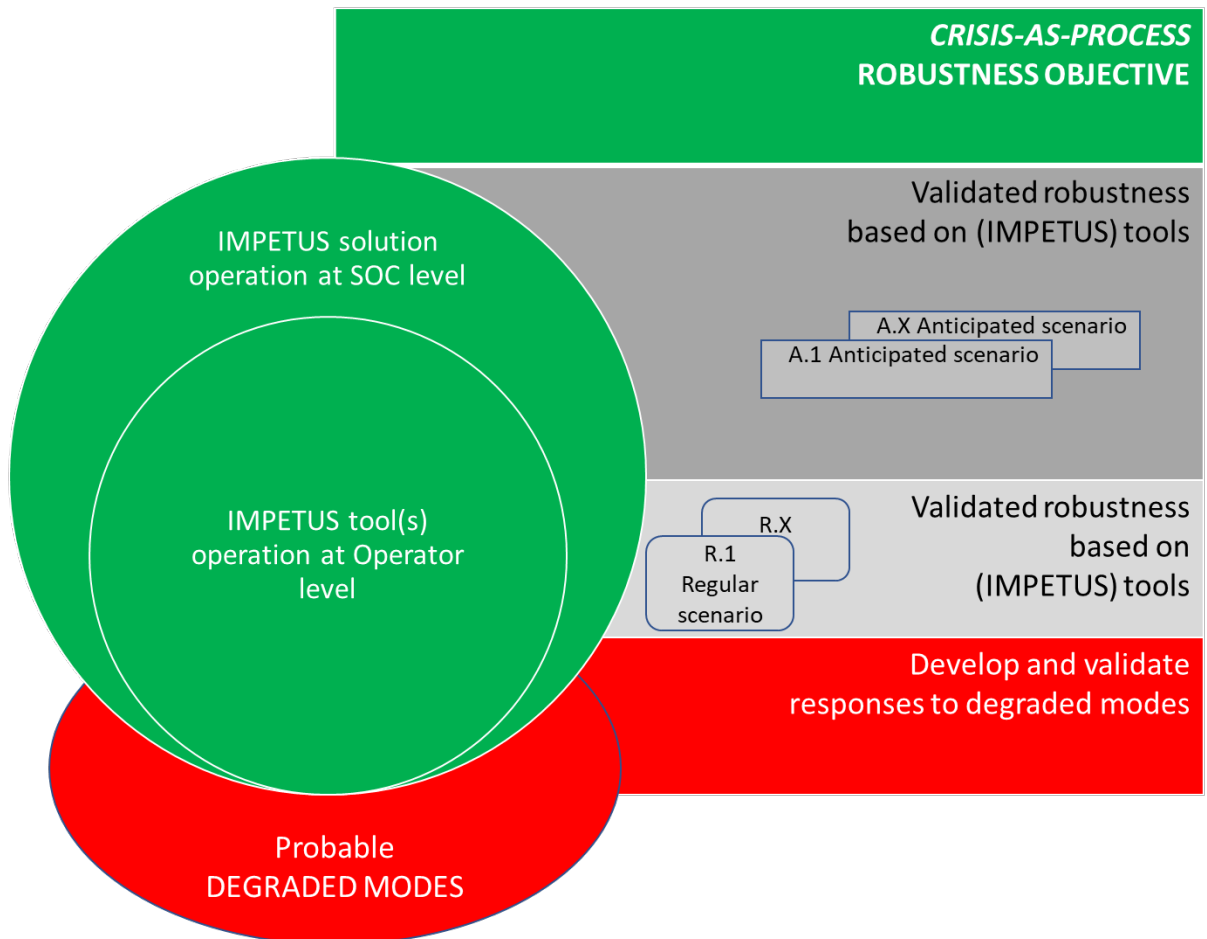
STRESS-TEST Robustness





The SOC should periodically stress-test the validated Robustness through a relevant Surprise scenario, encompassing the SOC as a whole. *Surprise scenarios should evolve based on prior results.*

STRESS-TEST Degraded Modes

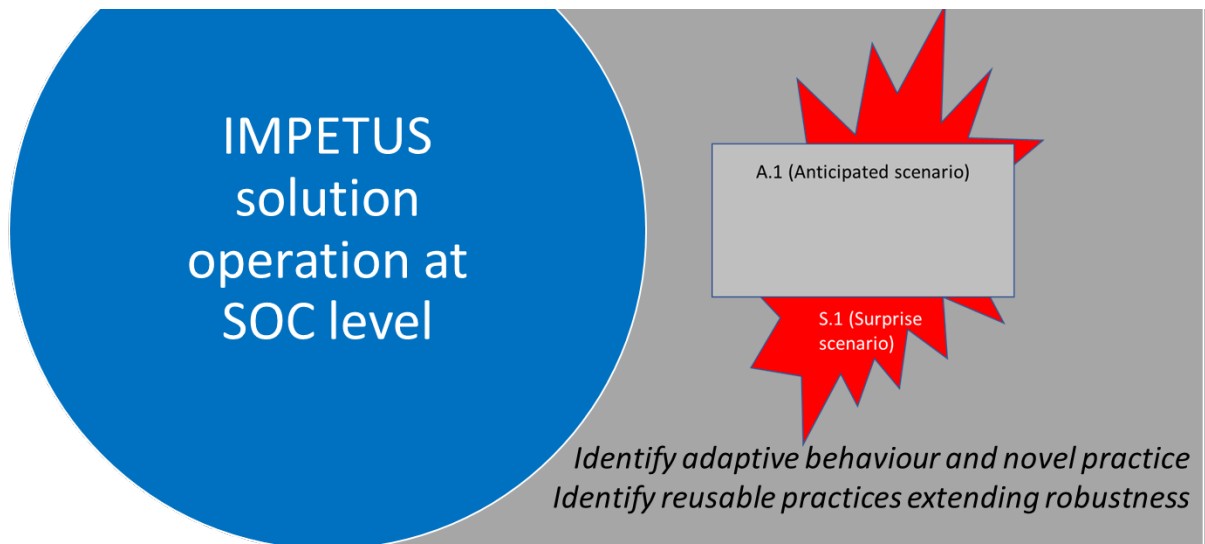


A special case of stress-testing should periodically be conducted on degraded modes. The degradation should be based on updated status of tools, their inter-connectivity, and their dependency on joint platforms (see [Degraded Modes](#)).

Building Resilience from Robustness

Experiencing Resilience





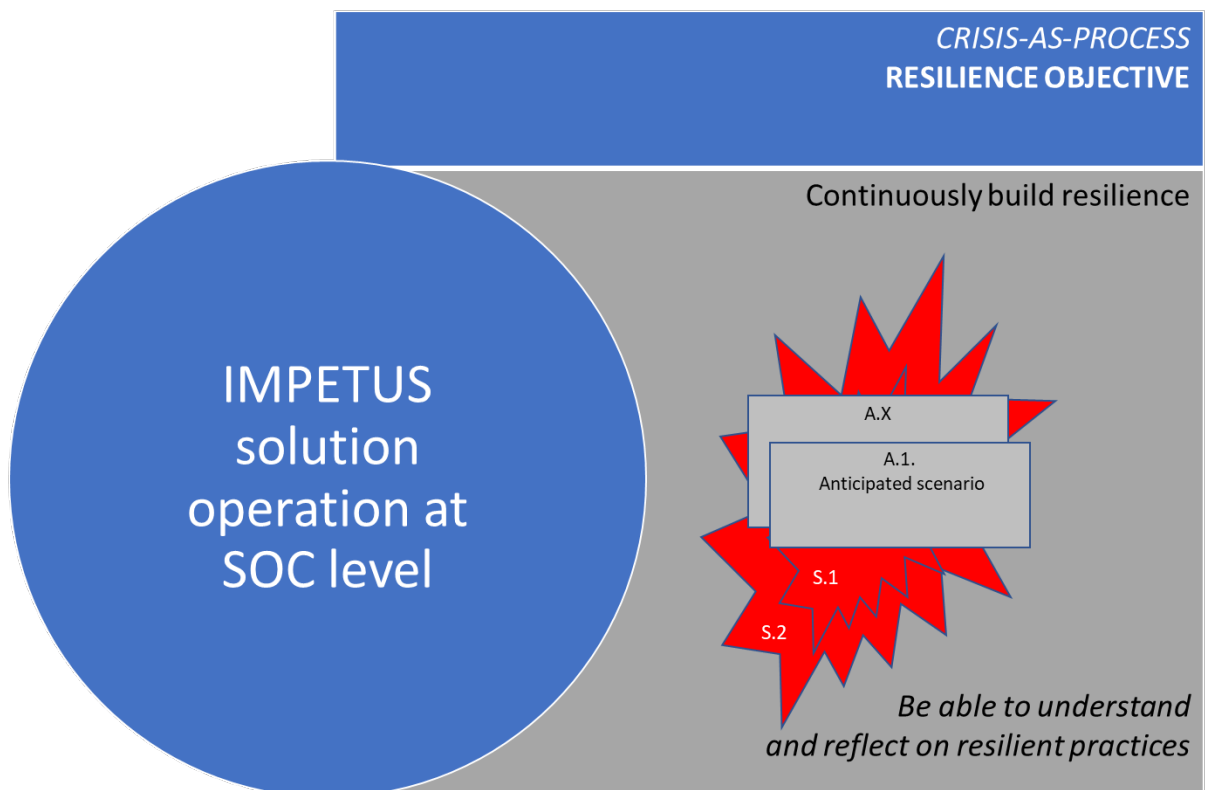
Based on the results from stress-testing of Robustness, a Surprise scenario should be calibrated that enables the SOC to develop novel solutions that subsequently can be used for joint analyses and reflection. The reflection process should have two different foci

1. What enabled the SOC to find a novel solution
2. Is the novel solution something that can be reused in a future situation, to the extent that it can be incorporated into operational procedures?

Surprise scenarios should continuously evolve to reflect advances in robustness, as indicated above.

This facilitates a crucial, dynamic link between Robustness and Resilience of the SOC

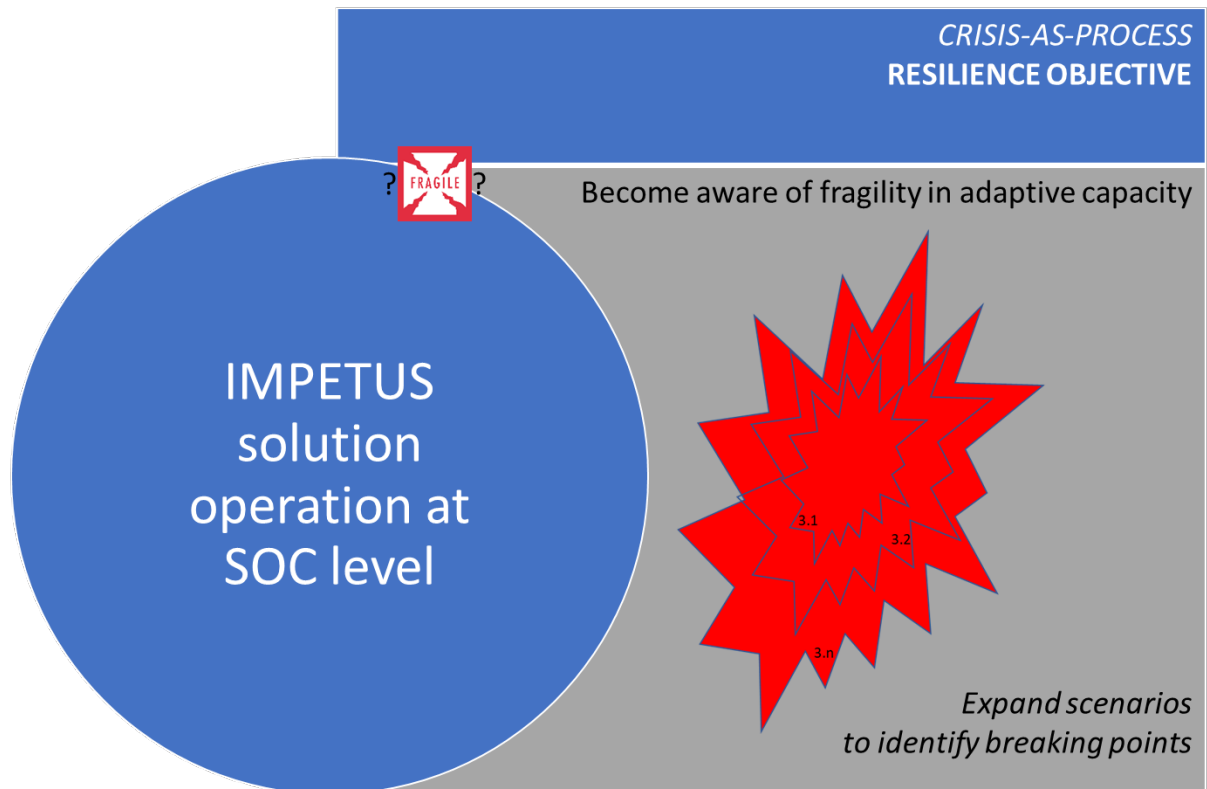
Expand Resilient Repertoire



Resilience must be constantly maintained and renewed. The SOC must therefore persist in renewing their perceptions of their own operational capabilities in terms of Surprise scenarios that represent the boundaries of preparedness.

This directs attention to their ability to manage their own adaptive *capacity*, rather than specific, imagined adaptations.

The DARWIN guidelines on *Managing adaptive capacity* is a useful resource. See [DRMG Book](#), chapter 3.



Also the *adaptive capacity may be fragile, causing a brittleness in operations*. When the SOC has reached the maturity level at which it is aware of and addresses its adaptive capacity, it is necessary to create awareness of its limitations.

Hence, Surprise scenarios which induces breakdown in adaptive capacity should be developed, with the intention of providing indicators of fragility when approaching these limits.

The DARWIN guidelines on *Noticing brittleness* is a useful resource. See [DRMG Book](#), chapter 4.3

Experiences

i In creating the Practitioners Guide on Operations, we hope that it will be actively used by people adopting advanced technological solutions (including, but not limited to, IMPETUS).

We have created this section (see the pages which follow) to provide a forum where we can gather "stories" from users who have considered adopting such technologies or have already started using them. By sharing and consolidating our practical experiences, we can learn from each other and make things easier for future adopters.

This section includes the following subsections:

[Tools and Their Impact](#)

[Challenges and Constraints](#)

[Utilisation of Potential](#)

Tools and Their Impact

This section will be filled with information we gather from readers on experiences related to:

- Direct benefits (and identified limitations) of individual tools
- Experiences on the direct impact of tools on working processes in SOC
- Assessments of the wider impact of tool adoption in terms of improving SOC performance, through experience-driven transformation, or strategic leverage

Challenges and Constraints

This section will be filled with information we gather from readers on experiences related to:

- Operator overload
- Gains versus brittleness in joint attention, awareness and sense-making
- Degraded modes

Utilisation of Potential

The generic relation between ensuring robustness and continuously building and renewing resilience in SOC operations is described [here](#).

This section will be filled with information we gather from readers on experiences related to:

- Ensuring robustness of SOC operations (advice on ensuring robustness is described [here](#)).
- Building resilience from robustness (advice on building and renewing resilience is described [here](#)).

Brief history of the Practitioners Guides

The development process of the Practitioners Guides is presented in the interactive presentation below. It outlines the concept, the different validation activities, and some of the major changes implemented during their development.

About IMPETUS

IMPETUS (Intelligent Management of Processes, Ethics and Technology for Urban Safety) is a Horizon2020 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 *practitioners 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 duration of 30 months and a budget of eight million euros.

This video from autumn 2021 gives an overview of the project and its main results. *A few details in the video are out-of-date (e.g. some tool names have been updated, some things presented as being in the future have now happened), but the overall message is accurate.*

IMPETUS partners

RESEARCH	INDUSTRY & SMEs	NGOs	CITIES
    	     	  	 

How might people responsible for safety and security in a city benefit from using a solution such as IMPETUS?

The technological solution provided by IMPETUS provides an example of advanced technology, partly based on AI (Artificial Intelligence) techniques, aiming to help improve safety in public spaces. Other specific tools and packages exist and new ones will surely emerge in future. They bring key benefits to a city:

- Deploying the technology can help you increase your city's resilience to various threats and improve crisis management.
- Using advanced information tools will expand the "ears" and "eyes" of your city, enabling early detection of impending problems.
- Improvements in operational decision-making can help prevent problems from escalating.

The [Practitioners Guides](#) developed in IMPETUS provide advice on multiple issues that need to be considered in the successful *deployment* of such technology, covering the proper handling of personal and other sensitive data, operational issues and cybersecurity. The lessons to be learned from the Practitioners Guides apply to use of any type of advanced technology for public safety - not just the specific tools developed in IMPETUS.

The IMPETUS solution

With its wide coverage, tight integration and validation through detailed testing in two pilot cities, IMPETUS can have an important role in convincing city authorities that practical application of such technology is feasible in the short and longer term. We invite you to learn more by looking at our [Description of IMPETUS Tools and Platform](#).

Copyright notice

Copyright © The IMPETUS Consortium

Copyright Notice

The IMPETUS Consortium hold copyright on the contents of the Practitioners Guides.

The material is made available under the terms of Creative Commons CCBY-NC-ND 4.0 licence <https://creativecommons.org/licenses/by-nc-nd/4.0/> which is defined as follows:

You are free to:

Share — copy and redistribute the material in any medium or format

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

NonCommercial — You may not use the material for commercial purposes.

NoDerivatives — If you remix, transform, or build upon the material, you may not distribute the modified material.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Authorship (for use when giving attribution under the terms of the Creative Commons licence)

The IMPETUS Consortium: European Commission Horizon 2020 Project "IMPETUS", grant number 883286 - <https://www.impetus-project.eu/>