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

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

http://www.impetus-project.eu

IMPETUS Project Deliverable: D6.5

Envisioning future evolutions

Dissemination Status: Public

Editors: Iris Cohen (THA), Wouter Hoogstra (THA)

Authors/Contributors:

Iris Cohen, Wouter Hoogstra, Thomas de Groot, Rafal Hrynkiewicz, Manon Tolhuisen (THA); Bruno Bonomini (CPAD); Ian Simon Gjetrang, Eirik Bærulfsen, David Røttingen (OSL); Mišo Mudrić, Jelena Radošević (ISP); Marco Anisetti, Claudio Ardagna (UNIMI) ; Michelangelo Ceci (UNIBA) ; Keren Saint-Hilaire, Sandrine Bayle (IMT); Joe Levy (CINEDIT); Alexia Comte (UdN/IMT), Axelle Cadiere (UdN) ; Maria Mirada, Guillem Garcia (INS) ; Paolo Mocellin, Matteo Bottin (UPAD); Sachin Gaur (BMA); Brian Holecek (TIEMS); Radu Popescu (SIV); Andrea Vik Bjarkø, Stine Skaufel Kilskar, Tor Olav Grøtan (SINTEF)

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

About IMPETUS

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

IMPETUS provides a solution that brings together:

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

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

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

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

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

The project started in September 2020 with a planned duration of 30 months.

For more information

Project web site: https://www.impetus-project.eu/
Project Coordinator: Joe Gorman, SINTEF: joe.gorman@sintef.no
Dissemination Manager: Harald Drager, TIEMS: khdrager@online.no

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

Executive Summary

The goal of this deliverable is to create awareness of trending technologies that are likely to impact the IMPETUS solution from different perspectives. Different impacts of the identified trending technologies are expected and described in this document.

First, trending technologies needed to be identified. For this purpose, interviews with stakeholders and webinars and workshops with tool partners were held. Participants talked about relevant technologies and the expected impact these technologies would have e.g., on their tool, or on the operational processes their organization is involved in. Several different perspectives on the impact of the technologies came to light. Based on the different expected impacts, the technologies were categorized as follows:

- impact on *the IMPETUS platform*,
- impact on *specific platform capabilities*,
- impact on *operational processes* around the use of the IMPETUS solution,
- impact on *separate tools* integrated in the platform,
- expected *negative use and impact*,

Further impacts were

- *societal impact* and
- *technologies foreseen for the future* (>5 years down the line).

Overall, the IMPETUS solution contains state-of-the-art techniques and technologies. But rapidly evolving or newly created or deployed technologies increase the need for constant development of the IMPETUS solution that is depending on the evolutions. Awareness is the first step to a resilient platform that is prepared to adopt or adjust itself for future evolutions.

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

Table of Contents

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

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

Table of Figures

List of Tables

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

List of Abbreviations

Table 1: List of Abbreviations

Abbreviation	Explanation
Tools	
SMD	Social Media Detection
FD	Firearm Detector
BD	Bacteria Detector
CTI	Cyber Threat Intelligence
UAD	Urban Anomaly Detector
WMS	Workload Monitoring System
EO	Evacuation Optimizer
CTDR	Cyber Threat Detection and Response
AI	Artificial Intelligence
BCI	Brain Computer Interface
DDoS	(Distributed) Denial of Service
ELT	Extract, Load & Transform
ETL	Extract, Transform, Load
RSA	Rivest–Shamir–Adleman (names of inventors of this public-key cryptosystem used for secure data transmission)
SA	Situation Awareness
SCSP	Smart City Safety Platform
SOC	Security Operating Centre
TRL	Technology Readiness Level
XAI	eXplainable Artificial Intelligence

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

List of Definitions

Table 2: List of Definitions

Term	Definition/explanation
ETL & ELT	*Extract*, *Transform*, *Load* is a process for data warehousing. Source data is extracted, transformed to useful form, and loaded into an access location. Most current ETL setups consist of a powerful server for the Transform and for the Load part of the equation. The ELT paradigm shift wants to go from Extract, and to Load and Transform in the same server, thus, being more efficient with resources.

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

1 About this deliverable

1.1 Why would I want to read this deliverable?

By reading this deliverable the reader will get awareness of the trending technologies that are expected to impact security and smart city solutions in the near future, as well as their impact on the directions for integrating these evolutions into the IMPETUS solution. New technological developments in the area of communication, security and other opportunities are described in relation to the platform and the operational processes it supports. This will help the reader get a sense of possible future steps for the whole IMPETUS solution.

Results from D1.2 (Requirements for public safety solutions), D5.1.2 (Ethical framework), D6.1 (Initial concepts of operations) and D6.4 (Operational framework – implementation guidelines) have a direct impact on the constraints and challenges of what is possible within the IMPETUS solution regarding the possible additional technologies and their integration.

1.2 Intended readership/users

The target audience of this document are people with an interest in smart cities, emergency response, citizen rights, government, and in research in the area of safety, security and ethics related to these topics. More precisely, the readership is intended for people who want to learn more about the future evolutions in technologies that are beneficial, or detrimental, to solutions for security and safety of public open spaces. Readers can broaden their understanding regarding the future of the IMPETUS solution and the impact it may have directly or indirectly on their work or their research. The deliverable provides insight and awareness on the impact of future technological developments on the IMPETUS platform, their operational processes, and legal and ethical aspects.

The reader should have a basic understanding of the IMPETUS project or platform, but a pure technical background will not be necessary. The readers would also benefit from an understanding of the different tools. The deliverables and publications that contain this and other information are listed in the next paragraph.

1.3 Other deliverables that may be of interest

For members of public organisations or citizen rights organisations the results described in ‘D5.1 Initial Ethical Framework’ and ‘D5.2 Initial mechanisms to preserve privacy in the secure smart city’ are relevant.

Readers who work in the area of emergency response might be interested in ‘D6.3 Operational framework – concepts of operations’ to assess what the IMPETUS solution could bring to their field.

For every reader the following deliverables could be of interest;

- D2.3 (Platform v2 release + APIs + documentation) to get an understanding of what the solutions are;
- D3.1, D3.4 and D3.7 (different tool development final reports) for a technical point of view on the modules;
- D4.2 (Data analytics, interface & access control final report) for an operational use perspective;
- D7.2, D7.3, D7.6, and the practitioners guides (acceptance pilot report, report on use of technical platform in pilots and use of the frameworks, and updated cyber vulnerability report) for details on acceptance, user and vulnerability of the IMPETUS platform.
- The Practitioner’s Guides on Ethics, Cybersecurity and Operations.

1.4 Synergy with other projects

Several EU research projects were identified to be relevant for this task as they focus on the same domain or part of the same domain and use or explore different technologies. The projects that use or explore relevant technologies are listed below.

7SHIELD is a H2020 funded research project. The 7SHIELD objective is to provide European Ground Segment facilities with a holistic framework to confront complex cyber and physical threats by covering all the macro stages of crisis management, namely pre-crisis, crisis and post-crises phases.

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

FASTER is a H2020 funded project which consortium consists of research, social and technical partners and first responder organizations. FASTER addresses the challenges associated with the protection of first responders in hazardous environments, while at the same time enhancing their capabilities in terms of Situation Awareness and communication.

MOSAICrOWN aims to enable data sharing and collaborative analytics in multi-owner scenarios in a privacy-preserving way, ensuring proper protection of private/sensitive/confidential information. *MOSAICrOWN* will provide effective and deployable solutions allowing data owners to maintain control on the data sharing process, enabling selective and sanitized disclosure providing for efficient and scalable privacy-aware collaborative computations.

S4allcities uses digital twins to create Situation Awareness. Their technology aims to revolutionize the way smart cities become more protected, prepared and resilient to both physical and cyber-attacks on City soft targets, smart spaces and critical infrastructure networks, by greatly augmenting City Spaces Situation Awareness with intelligence, context and evaluated real-time cyber and physical security threat levels.

Select 4 cities stimulated research and development of city-wide Internet-of-Everything platforms. The SELECT project started a competition open "*to all European companies to develop an open, standardized, data-driven, service-oriented and user-centric platform that enables large-scale co-creation, testing and validation of urban IoE applications and services*".

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

2 Identifying future technologies – approach

Several different methods were used to collect input and data for this deliverable. Methods included interviews with stakeholders, workshops with tool partners, a survey for project partners, and webinars. The following sections provide a description of the different methods used and gives an overview of the overall approach.

2.1 Input collection from stakeholders and tool partners

At the start of this task, initial interviews were held with the cities. These interviews aimed at identifying technologies that are currently used by the cities, and technologies that are expected to be used in the near future and how they will have an impact on the cities. Furthermore, we asked what kind or result of this task would be beneficial for them.

The city of Padova made it clear that it is important to consider the opportunities and challenges offered by future technologies but also to consider the impact on the operational processes. At the start of the project, the main IMPETUS end-user was thought of to be the Security Operating Centre (SOC) operator. Further into the project, however, it became clear that more actors will be involved in the operational processes (both on the planning level and on the execution level) concerning IMPETUS. The roles that can now be identified at the planning level are; strategic planners or city executives, and at the execution level, the identified roles are: SOC operators, SOC supervisors, IT department specialists, IT department supervisors, intelligence analysts (e.g., judicial police) and technical administrators. When considering the impact of future technologies (especially on the operational processes) we tried to take into account all identified roles working with the IMPETUS platform.

The city of Oslo stated a clear goal on what they want to achieve with the platform now and in the future. The platform should improve their Situation Awareness (SA) of incidents and during events and optimise how they can manage these incidents with their end-users. This should be the focus of any newly introduced technology.

After the initial interviews with Oslo and Padova, workshops were scheduled with the different tool partners. During these workshops, the tool partners were asked to describe their tools, what opportunities they foresee for their tools regarding new technologies, and what the impact of these technologies will be for their tool and for the IMPETUS solution. Three workshops were planned in which two tool partners were invited. During the first workshop, partners working on the WMS and CTDR were present, during the second workshop partners working on the BD and UAD were present, and during the third workshop partners working on the SMD and EO were present. Other forms of input collection needed to be used for the tool partners that could not be present during the workshops. In those cases, mainly email contact was used.

The workshops were roughly following the same structure:

Introduction of:

- Workshop moderators
- Workshop participants
- Brief introduction of the tools (by the tool partner)

Identifying technologies:

- Opportunities for each tool (near future). The tool partners were asked to provide their insight. If none were given they were asked to explain if they saw relevance of previously mentioned technologies on their tools. In a few cases, the tool partner could not provide such technologies or had to be very generic in the technologies for various reasons. This is reflected in the next chapters in less input and in the tables.

When a technology was mentioned, it was directly placed on the Mind map, and further questions were asked to **gather information about**: expected impact on their tool, the operational use, expected impact on the IMPETUS platform as a whole.

During the workshops we used an online whiteboard-tool called Miro. The three Miro boards from the workshops are added in the appendices of this document.

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

2.2 Input collection from related EU research projects

The IMPETUS project kept track of relevant EU research projects, organisations, consortia or initiatives, that focus on similar topics as the IMPETUS project. Further relevant technologies were identified with the use of the websites and dissemination material of these organisations.

As a first step, every website including the public deliverables and dissemination materials of all relevant organisations were analysed. During the analysis, we searched for mentioning of technologies that were used by the organisation within a new framework, we searched for mentioning of newly developed technologies by the organisations, and we searched for mentioning of technologies on which the project relies in other ways. Five projects focussing on supportive technologies for first responders (FASTER), technologies against cyber- and physical threats (S4ALLCITIES and 7SHIELDS), technologies for protecting shared data for collaborative analysis (MOSAICrOWN), and on specific IfE technology (Select4Cities) (see section 1.4) clearly mentioned technologies and how they are used within their project's scope.

As a first filtering step, the editors who performed the analysis considered the relevance of the technology for IMPETUS. Some of these technologies were already mentioned by IMPETUS tool partners during the workshops; the other technologies were further analysed on their relevance to IMPETUS. Whether or not a technology was relevant is inherently subjective and influenced by someone's imagination, experience, knowledge and background on the subject matter. We therefore tried to let this decision ('relevant for IMPETUS or not relevant for IMPETUS') be decided by the experts in that specific field. For this purpose an online survey was created. The survey is added to appendix 9. In this survey the experts could indicate if a technology would be relevant and meaningful to IMPETUS, and what they expected to be the impact of these technologies. The results were used as direct input for the deliverable, or to guide the text needed to be written by the editors for sections in the deliverable.

2.3 Categorization of identified technologies

After all stakeholders had been heard, the identified technologies were structured for a clear presentation in the deliverable. Several categories related to the expected impact could be identified. Those categories are:

1. Impact on the IMPETUS platform,
2. Impact on specific capabilities of the IMPETUS platform,
3. Impact on specific operational processes within the IMPETUS operations,
4. Impact on specific tools within the IMPETUS solution,
5. Technologies expected to be used in adversarial ways.

Further impacts that were discussed in a broader sense;

6. Societal impact on technologies and vice versa,
7. Impact on ethical and legal issues,
8. Far future impacts; technologies that reach high maturity after 2030.

As category 8 indicates, the main focus of our analysis was on technologies that would be high in Technology Readiness Level (TRL) before 2030. This was a difficult criterion to estimate, therefore, all tool providers were asked in the survey to indicate if they saw the certain technologies to be operational before or after 2030.

2.4 Summary

Several different methods and steps were needed to create a complete list of relevant technologies for this deliverable. Input came from tool providers, partner cities and the websites of related EU research projects. The collected technologies were structured in categories related to their expected impact. The next chapters will provide descriptions of the technologies. The expected impacts (positive and negative) are provided in tables, focussing on the different categories mentioned above.

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

Note that the following chapters do not contain an explanation of all technologies expected to enter high TRL by 2030. Only the technologies identified using the approach described in this chapter are incorporated. An overview of all identified technologies is shown in Figure 1.

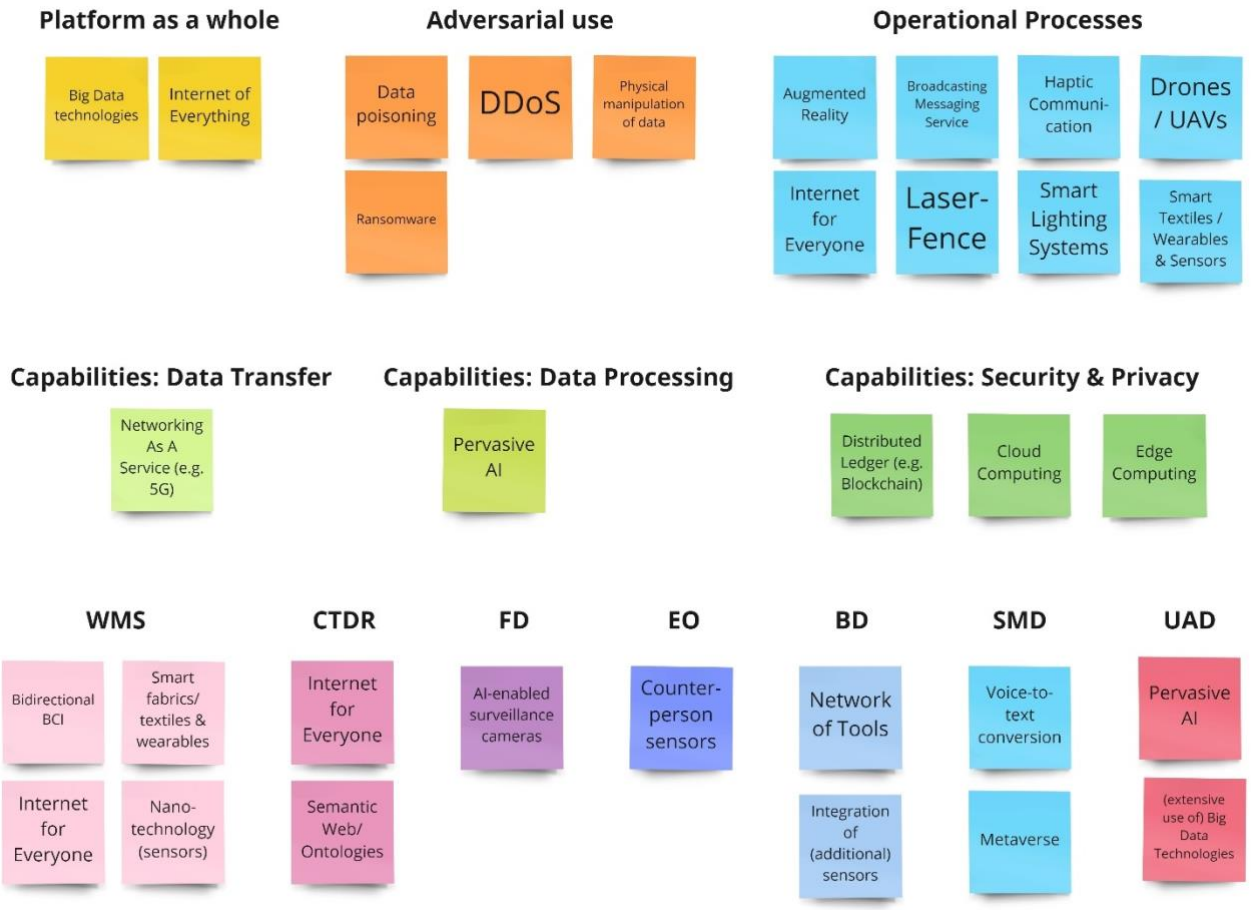


Figure 1. Overview of all identified technologies, categorized on their expected impact.

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

3 Impact on the IMPETUS solution

This chapter provides an overview of the envisioned technologies that have an expected

1. Generic impact on the IMPETUS platform as a whole (see 3.1),
2. Impact on specific capabilities of the IMPETUS platform (see 3.2),
3. Impact on specific operational processes within the IMPETUS operations (see 3.3),
4. Impact on specific tools within the IMPETUS platform (see 3.4),
5. Negative impact from technologies used by adversaries (e.g. technologies for criminal use) (3.5),

It is important to note again that only technologies that have been identified during the input collection as described in the previous chapter are included in this overview. Hence, technologies mentioned here are not a complete list of future technological evolutions.

3.1 Identified technologies impacting the IMPETUS platform and its capabilities

The technologies described in this section are expected to have an impact on the IMPETUS platform as a whole. The IMPETUS platform revers to the combination of tools and User Interface that is the result of the IMPETUS project. The expected impacts are collected in Table 3.

3.1.1 (Extensive use of) Big Data technologies

The current trend in data analytics suggests that in the near future the data will be more and more heterogeneous and available at different granularity levels, with different speeds and veracity. The sensitivity of the data will also become a more severe problem given the capillary diffusion of pervasive data sources. ELT paradigm (Extract, Load & Transfer in the same server) will overcome the ETL (Extract, Transfer, Load, architecture) due to the increasing need for shared data to be fed into AI-empowered services. Big Data ingestion architectures such as the one currently adopted in IMPETUS will need to be adopted more diffused, especially in the smart city context to control the data quality, sensitivity, and granularity of each service. The ingestion pipeline will rely on edge-to-cloud continuum connectivity enabling seamless data gathering procedures.

Data sharing among tools and the user interface dashboard, within organizations and among different stakeholder, is a big bottleneck in smart cities. In order to adhere to privacy guidelines there is a big push for a federated learning approach for AI models and a privacy driven approach of sharing the final decisions instead of the sharing the data. This would imply running the model on the edge rather than sending data to the server.

There is a need for a middleware to overcome the heterogeneity of data sources and streamlining the access upstream for application developers and for the purpose of innovation. Standards like oneM2M (oneM2M, n.d.) and NGSI LD (Zangelin, 2020) have been created to cater to this need. They provide a well-documented API to the middleware which is independent of the IoT sensors and vendor hardware. So, the cities are free to develop applications, dashboards and replacing vendors become easy ensuring interoperability, security and better return on investments. We already see global adoption of these standards and city level provision, of middleware in providing streamlined access and guaranteeing privacy and security of data assets (India Urban Data Exchange (IUDX) 2022).

3.1.2 Internet of Everything (IoE) (Source project: *Select 4 Cities*)

The Internet of Everything differs from the Internet of Things, in a way that it addresses more than just the physical objects in the world. The IoE aims to connect people, things, data and processes.

The independent devices of the past are now being connected to the Internet including machine-to-machine (M2M), person-to-machine (P2M), and person-to-person (P2P) systems." (Miraz, Ali, Excell & Picking, 2015)

3.2 Identified technologies impacting specific capabilities of the platform

This section lists the technologies that are expected to have a relevant impact on specific capabilities of the IMPETUS platform. Their impact is expected to improve the **security and privacy** of data logging (e.g.

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

blockchain) and improve the speed of **data transfer** (networking as a service, e.g., 5G). The expected impacts are collected in Table 3.

3.2.1 Improved security and privacy

Technologies in this section are expected to have a positive impact on the ability of the IMEPTUS platform to provide security and privacy in some form. The expected impacts are collected in Table 3.

Distributed Ledger (e.g., Blockchain)

"A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically through the use of keys and signatures to control who can do what within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network." (Distributed Ledger Technology, 2022)

Cloud computing

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Cloud computing definition, 2011)

Edge computing (e.g., Fog computing).

All computing that is taking place outside of the cloud, and at the edge of a network is considered edge computing. It processes data in real-time, using data instantly generated by sensors or users. Edge computing is a distributed computing paradigm and can be defined as an architecture rather than a technology.

Where centralized computing is limited by e.g., latency, bandwidth, data privacy and autonomy, having the processing taking place closer to the data source, edge computing is not limited by those factors (Gartner, 2020).

3.2.2 Improved data transfer

Technologies in this section are expected to have a positive impact on the ability of the IMEPTUS platform to transfer data. The expected impacts are collected in Table 3.

Networking as a service (NaaS, e.g., 5G).

"NaaS is a cloud model that enables users to easily operate the network and achieve the outcomes they expect from it without owning, building, or maintaining their own infrastructure. NaaS can replace hardware-centric VPNs, load balancers, firewall appliances, and Multiprotocol Label Switching (MPLS) connections. Users can scale up and down as demand changes, rapidly deploy services, and eliminate hardware costs." (CISCO, 2022)

5G is the 5th generation mobile network. It is a new global wireless standard after 1G, 2G, 3G, and 4G networks. 5G is characterized by a larger data transfer and less latency compared to its predecessors. According to the European Union's digital strategy, the target for 5G coverage is to cover all populated areas with 5G by 2030 (5g, 2022).

"CISCO expects that 5G will be much faster than today's networks but it will also be more reliable, more energy-efficient, capable of delivering high connectivity density and operating with very low latency. Using 5G's network slicing capability is a means of providing a differentiated experience for users and devices based on the specific requirements of the environment they operator in. Together with the […] new radio capabilities,

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

slicing will offer the service levels, security, controllability, programmability and uptime that are needed for challenging and even mission-critical applications today. Network slicing leverages the virtualization of mobile network resources to allow the operator to create many logical networks with unique capabilities over a single physical network. With 5G, the dynamic provisioning and scaling of network capacity and resources are available for the first time. The vision of managing the network-as-a-service in the same way as an application developer might manage cloud resources [..]." (CISCO2, 2022)

3.2.3 Improved data processing

Technologies in this section are expected to have a positive impact on the ability of the IMEPTUS platform to process data. The expected impacts are collected in Table 3.

Pervasive Artificial Intelligence (AI)

In future applications AI algorithms will be more and more embedded in all devices and sensors around humans and their environment. This phenomenon, typically called pervasive AI, requires a more advanced, more distributed use of AI and includes edge computing (*see*: edge computing in 3.2.1) of the AI technique locally.

However, pervasive AI requires new hardware and software technologies. From the point of view of AI, it requires new meta learning techniques. Meta learning has been investigated for many years, but the combination with edge computing and pervasive AI is still not mature in the literature. Another aspect that could support pervasive AI is represented by the application of transfer learning techniques. Such techniques learn models for some target domain, by exploiting information coming from both the target and a different, but related, "source" domain. In pervasive AI, this would give the opportunity to learn a local model by re-using information embedded in other local models.

The adoption of such techniques in pervasive AI would provide as secondary effect the possibility of a better scalability that gives the opportunity to process more data and better understand the phenomena under analysis. This is strictly related to causality: a better understanding of the environment does not only provide information about correlations, but also about cause-effect relationships. In addition to causality, another aspect that could be helpful to the final users is eXplainable Artificial Intelligence (XAI), where the idea is to provide interpretability of decisions taken by AI techniques. Although in IMPETUS some work has been done in the direction of XAI (see, for instance, the feature ranking of the anomaly detection in the UAD tool), pervasive AI would require much more effort in this direction.

Table 3. Technologies impacting the platform and specific platform capabilities

Technology	Expected positive impact on IMPETUS platform capabilities	Expected challenges and constraints
Whole platform		
(Extensive use of) Big Data	This scenario where the data lake has a central role and is fully under the control of the Big Data engine, will enable the outcomes of smart cities services such as the ones of IMPETUS tools; thus, extracting advanced knowledge and providing decision support for users.	
Internet of Everything (IoE)	In theory, IoE will make it possible to access all the data. This could improve the scope and reliability of any tool that makes use of the social media for example, as well as any cyber-	The more data is shared, the more vulnerable any institutions or organizations using the IMPETUS platform will become; leading to the need for

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

Technology	Expected positive impact on IMPETUS platform capabilities	Expected challenges and constraints
	threat related tools, which could collect more and different information. In addition to more opportunities for sensor placements and type of sensors deployed on the various locations, it also has edge computing opportunities in terms of using cell phones as sensors. This is particularly relevant for service phones for security organisations where you can deploy protected environments around the sensors. I.E portable AI cameras that can provide various types of information, sound analysis, accelerometers etc for various types of information during situations. Other opportunities are deployment of temporary sensor arrays for events i.e., or collection of information through various sources of sensors already existing, i.e., "every fridge has a camera" that can be used to detect events as home invasions and be incorporated into alarm systems.	more, or more elaborate, tools to protect themselves. All this will also have ethical and legal implications as well; the issue of the personal and sensitive data will become even more complex, since one will be able to identify and localize an individual from the patterns in seemingly non-personal data. On the other hand, the general population also have a lot to contribute with if they voluntarily provide information and perhaps in situations like kidnappings it could be decisive in solving the situation.
Security and privacy		
Distributed Ledger (e.g., Blockchain).	The objective of this technique is secure logging. Blockchain can be used for storing information which allows for the secure preservation of evidence because it ensures there is no manipulation of the information. Blockchain will mainly affect the post-event operational processes; it allows for a thorough tracking of the decisions process performed before and during an event by the different roles involved in the process. Debriefing of an event, and audit of an event become more secure.	A negative impact is that more complex infrastructure is needed. More people need to be hired to maintain this infrastructure.
Cloud computing	Cloud computing or cloud service is making services, hardware, software and data available on request via a network – often the internet. Although it is already used by the SMD tool, other tools such as EO, see that this technique can be beneficial in the future. For EO, the baseline simulations are heavy to compute. Cloud computing could provide new simulations based on new data (or historical data) coming from sensors. Other uses of cloud computing are foreseen in the context of image processing. For large events, ad-hoc cloud resources could be used to process all the image data for the search of weapons. When the processing can be	When deployed in this manner, another negative impact is identified; the data transfer needs to be encrypted to ensure security and privacy. Using cloud computing to provide simulations and models to the EO tool, brings another negative impact namely that the simulation models could be incorrect or not as correct as necessary. If that is the case, the EO outcome will differ from the actual situation.

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

Technology	Expected positive impact on IMPETUS platform capabilities	Expected challenges and constraints
	anonymized, this task could be assigned to cloud resources. For the EO the baseline simulations are heavy to compute. Cloud computing could provide new simulations based on new data (or historical data) coming from sensors.	
Edge computing	City-wide IoT networks are the next innovation in smart cities. In principle, they are built upon a high bandwidth, low-latency network capable of handling big data, but currently, at least until reliable and affordable 5G becomes more commonplace, network connectivity can be lacking. Edge computing is the answer. Traditional IoT networks collect and analyse data before sending it to a central cloud computer, where it can be processed and acted on. Edge computing, meanwhile, allows for more on-device computing and analytics. Furthermore, it saves on the round tripping to the server and in some cases, it is cost efficient as there are no cloud computing costs. It is also good for use cases where data is sensitive and should not be shared with third parties.	It could also have a negative impact in terms of security due to actual limitations of current edge technologies.
Data transfer		
NaaS (Networking as a Service) e.g., 5G	The overall benefits of NaaS are simplicity in IT and in hardware and software management. It will provide greater speed, agility and scale. 5G is faster and can connect more devices than existing networks. This is a benefit for other technologies and concepts such as the Internet of Everything. Quality of internet services is improved even with a large number of users in crowded areas.	Almost all 5G hardware infrastructures belong, currently, to a limited number of suppliers not all always fair in terms of public safety (e.g. risk of spying)
Data processing		
Pervasive AI	Expected to provide better scalability that gives the opportunity to process more data and better understand the phenomena under analysis.	Requires new hardware and software technologies. From the point of view of AI, it requires new meta learning techniques.

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

3.3 Identified technologies impacting operational processes

This section describes the technologies that are expected to impact operational processes of the different IMPETUS (end-) users. The expected impacts are summarized in Table 4.

In terms of SOC personnel, impact on all four basic processes (i.e., information collection, information analysis, response activation, and response evaluation and correction) is considered when relevant. So are aspects influencing the operational capabilities of the SOC as an entity. These include increased awareness of the operators' role, joint understanding and SA, enhanced decision-making, new operational patterns utilizing new information pathways, changes in communication patterns, and common operational language (IMPETUS, 2022).

It should however be kept in mind that for the assumed capabilities of the SOC as an entity, the presumed impact requires a thorough organisational development and calibration process that cannot be addressed here. Nevertheless, a potential for both enhanced robustness and resilience of SOC operations can be envisaged, but also a potential brittleness.

Augmented Reality (AR) (Source project: *FASTER***)**

Augmented reality provides a real-time view of the physical real world that has been enhanced or augmented with computer generated information (Arregui-Vicomtech, 2021). It is typically provided through head-mounted displays, AR glasses, head-up displays but can also be projected on video images of a tablet screen.

Broadcasting messaging service

Broadcasting services such as the cell broadcasting technique, provide the ability to send one single text message (an SMS) to thousands of people at the same time by targeting cell phone numbers in a certain geolocation. No prior knowledge of the phone numbers is necessary.

Examples of broadcasting messaging services already in use in Europe are EU-Alert (EU), FR-Alert, NL-Alert, LT-Alert, RO-Alert, GR-Alert.

Haptic communication (Source project: *FASTER***)**

Haptic communication can be applied through a variety of devices. For example, wristbands can communicate information to the user via haptic feedback (e.g., vibrations) in settings where auditory and visual information cannot be provided. Furthermore, smartwatches can be used to record and identify the users' arm movements. These can be used to communicate information without having to speak or type which lets the user keep looking at the environment.

Drones, Unmanned Aerial Vehicles (UAVs) and other multi-functional autonomous vehicles (COSSEC projects: *FASTER, 7Shield***)**

Drones or UAVs are aircrafts operated without a human pilot on-board the vessel. A human could operate an aircraft from a remote-control station which would be the case with Remotely Piloted Aircraft. When no pilot is involved, the UAV becomes an autonomous UAV. Vehicles not leaving the ground that function autonomously are called multi-functional autonomous vehicles.

According to Vodák et al (2021) UAVs are listed as one in twelve advanced technologies that are used to manage smart cities, highlighting examples of use such as crowd monitoring and transport of medical supplies. Moreover, in a smart city surveillance setting "UAVs can serve as internet of things (IoT) devices for data sharing, provide real-time data for input into 'big data' applications, and enable efficient decision-making [2]" (Gohari et al., 2022; Ayamga, Akaba, Nyaaba, 2021).

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

Internet for Everyone (IfE)

Internet for Everyone, is the idea of connecting the last billion people on earth that do not have a (reliable) internet connection at hand, to the internet. Geographical challenges, or natural disasters can be reasons for an area to not be connected. Overcoming such issues will allow for wireless connectivity to the internet for everyone on the planet (Katikala, 2014).

Laser Security System (e.g. Laser-Fence) (Source project: *7SHIELD***)**

"*Laser is a device that emits light using a process called optical amplification which is based on stimulated emission of electromagnetic radiations. […] It is used in various fields which consists of military, medical and technological spheres*" (Goel et al., 2022). In the EU Horizon-project 7SHIELD "*2D & 3D laser-based technologies for detection of ground-based intrusions by humans and vehicles, and aerial intrusions by drones*" (Pothrat, X, 2020) was suggested as a possible use of laser security system technology in protecting critical infrastructure.

Smart Lighting Systems (Smart Lighting System)

In Smart Cities, the lighting systems can be integrated with sensors (light, motion etc.) and communication channels, resulting in a Smart Lighting System (SLS). Such systems control the light intensity coming from the light unit in a flexible manner. SLS main goal is an autonomous and more energy efficient lighting management system that can result in reduced power consumption in indoor and outdoor settings (Sikder, et.al., 2018).

Smart Textiles / Wearables & Sensors (Source projects: *FASTER, s4allcities***)**

Smart textiles are pieces of textiles that are worn by their user and are incorporated with sensors. The sensors can keep track of bodily functions of the person wearing them (e.g., body temperature, heart rate, saturation), but they can also track environmental conditions (e.g., air temperature, air humidity, oxygen content, carbon monoxide content or to detect the presence of poisonous substances).

Wearables, or other wearable sensors, are stand-alone sensors that can be worn by the user, such as a smartwatch, or chest-belt. The wearable sensors are not integrated into a textile but can be used to measure similar conditions (bodily functions or environmental conditions).

Both smart textiles and wearables could also be used to communicate with the person wearing them (see haptic communication).

Table 4: Technologies and their expected impact on operational processes

Technology	Expected positive impact on operational processes	Expected challenges and constraints
AR	This technology is expected to impact the information collection and response activation processes. Certain use cases in the safety domain where AR can be of great benefit are the visualization of safe evacuation routes to the user, providing information such as a geolocation of units on a 2D map, or the marking of dangerous zones.	The placement of the information in the users' field of view needs to be thoroughly examined to prevent the AR information blocking the view of important objects or views in the real world. Also, the amount of additional information through the use of AR must be carefully considered in order to avoid information overload to the user.

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

Technology	Expected positive impact on operational processes	Expected challenges and constraints
	Further benefits of using head-mounted, or face-mounted AR (e.g., glasses), is that it provides hands free viewing of the information. Overall, it can provide better SA and a smoother operational process by providing relevant information in a hands-free way. It can contribute to joint understanding and SA as the same computer-generated information can be provided to several actors.	
Broadcasting messaging service	This technology is expected to impact the response activation process. The technology can be used to communicate to the citizens. During the 'response activation', broadcasting messages can be used as an alarm or instruction for citizens.	This might need some form of standardization of communication. Messages cannot be longer that a predefined number of characters.
Haptic feedback	This technology is expected to impact the communication patterns and information pathways in the field and in the SOC. It will also have an impact on the response activation process. This type of communication is more versatile in its deployment. Screens and phones cannot be used all the time in the field, e.g., when users need to communicate hands free, or when there is too much environmental noise. This technology has the potential to enhance the joint understanding and SA.	For communicating in both directions, the user needs to learn a new language; specific arm or hand movements translate into specific commands or request. Also, the amount of additional information through the use of haptic feedback must be carefully considered in order to avoid information overload to the user. The technology will lead to a new communication pattern which will necessitate development of a common operating language in order to avoid misunderstandings.
UAVs/drones	UAVs or drones can be used for observation through the city and thereby contributing to the 'information collection' phase of the operational process. It can also impact communication patterns, information pathways and decision-making processes depending on who receives and assesses the drone footage. Drones get the big picture of a site after an event. For example, after a mudslide a drone can detect risk and thereby reduce risk for emergency personnel, intervention unit. This may also increase the SA and enhance the decision-making of the SOC personnel since they perceive more information about the event.	Restrictions on drone use need to be considered, e.g., drones cannot fly close to an airport or certain public areas. The category of the drone (open, specific or certified) needs to be taken into account. For the specific category the operator needs additional safety training, or a certificate conform and perform a risk assessment according EU regulations. (EASA, 2021). The use of footage from drones might add to the total amount of information that a SOC-operator is exposed to and can lead to information overload. If misused, drones can be used to conduct both physical attacks and cyber-attacks.

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

Technology	Expected positive impact on operational processes	Expected challenges and constraints
		There are also privacy concerns connected to the use of drones for surveillance purposes (Vattapparambam et al., 2016). This possible new venue for cyber-attacks would be a concern for the IT personnel operating the IMPETUS platform.
IfE	This technology might impact the response activation process and influence communication patterns. Having more reliable internet connections, even in remote areas, will provide greater access for workers such as in-field emergency responders. It is also beneficial for communication with populations regarding evacuation and securing of areas. Furthermore, IfE is particularly important for developing countries, which are, at the same time, less resilient to security issues. Therefore, we see the greatest need to develop the internet for everyone project to bring the technology developed in IMPETUS to the cities that need it most.	The relevance is lower in Europe due to high connectivity, but for deployment outside of EU the relevance can be higher in this regard. When deployed outside the EU, other ethics and privacy regulations apply. When more data is available, more storage and processing capacity is needed. Users utilising IfE might be more vulnerable to cyber-attacks due to the use in developing countries which are less experienced with cyber security. This would be a concern for IT personnel operating the IMPETUS platform.
Laser Security System	This technology might impact the information collection/monitoring process and the response activation process. It enables improved detection of intrusions and thereby increases the monitoring efficiency. It has a high probability of detection, low probability of false alarms and nuisance alarms. If thought of as a checkpoint, UAD could make use of multiple laser points to understand movements of people from a mobility point of view. This can have potential to expand upon as a part of the EO toolset to understand evacuation situations and real-time situational awareness both before and during evacuation situations.	This technology needs to be either incorporated into an existing tool, or a new tool needs to be developed and implemented into the IMPETUS platform. This additional technology might add to the total amount of monitoring work that a SOC operator has to perform simultaneously and thus might affect the attention span. This will depend on how this technology is integrated with the other functions of the platform and whether it adds to or replaces other functions.
Smart Lightning	In the ‘response activation’ phase, this technology can be used to direct citizens towards a safe location. It could be used to light up areas where a threat is detected thereby leading to increased SA. It could also be used to shut off lights in certain areas order to deter a hostile activity.	The response towards certain lighting changes must be known by the citizens. A public campaign or other form of training/education is needed. If the technology is misused e.g., by hostile actors via a cyber-attack, the technology can be used to hamper the response to a critical event. This would be a concern for IT personnel operating the IMPETUS platform.

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

Technology	Expected positive impact on operational processes	Expected challenges and constraints
Smart Textiles / Wearables & Sensors	This technology might impact the awareness of the operator's role and the decision-making processes. These sensors can monitor the users' physical states (and extract mental states) and monitor environmental conditions in the field. It has the potential to lead to enhanced decision-making for supervisors and to enhance the awareness of the operator's role.	Humans need to accept them and wear them. Operators might become less aware of their own physical/mental limitations in situations of stress since technology is detecting it for them on a regular basis. Similarly, supervisors might become too dependent on technology to detect the state of their employees. This could be a concern in situations where the technology fails. There could be privacy concerns related to the data that is collected about the operator's physical and mental states. This data could be misused if the data is not properly secured.

3.4 Identified technologies impacting a specific tool

During workshops held with the tool providers, technologies were discussed that impact specific tools. Positive or negative impact will seep through to the IMPETUS platform, although an overall impact was not discussed. These technologies are described below, and their impacts are summarized in Table 5.

AI-enabled surveillance cameras

Surveillance cameras that are enabled for AI-algorithms come in various forms. It can be body worn cameras, drone cameras or standard CCTV cameras.

Also see: **Smart Textiles / Wearables & Sensors** in section 3.3.

Bidirectional Brain-Computer Interface (BCI)

Bidirectional Brain-Computer Interfaces are defined as devices that can communicate with a brain, to enable a two-way interaction between the brain and the environment. Current bidirectional BCI devices record and translate neural activity into motor commands, and sensory information from the environment is directly delivered into the brain. The most common use case for such devices is the application for patients with loss of motor skills. (Boi, et.al., 2016).

The global objective of such technologies is to help the system to understand the human it’s interacting with.

Counter-person sensors

Although still an emergent technology, there are several ways to digitally count people. Three people-counting techniques are mentioned by Terabee (How people counter sensors work: a tech comparison, n.d.): CCTV and stereo vision are used to optically count people, signal tracking is used to count WIFI device and thereby counting people, and time-of-flight sensors use infrared to count people.

Keeping track of numbers and flows of people is essential for Smart Cities to gain a full Situation Awareness of the location and situation and the occurrence of triggering events that induce a movement of crowds. Knowing

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

where the crowds are getting too large or where crowds are standing still can for example help security operations during large gatherings and events.

(Extensive use of) Big Data technologies

Objective: to control the data quality, sensitivity, and granularity of each service.

Also see: section 3.1.

Integration of additional sensors

Increasing the number of sensors into a system will result in more data for more precise sensing of the environment. Sensor integration can be loosely defined as: “the art of processing data from multiple sensors with an aim to replicate a physical environment or induce intelligence to control a phenomenon with increased precision and reliability" (Morales-Herrera, et.al. 2017) Data from multiple sensors must be integrated correctly to come to one outcome.

Objective: adding additional sensors to the tool will result in more collected data.

Internet for Everyone (IfE)

The objective of this technology is to establish a proper internet connection for everyone. Connecting the last billion users in rural area or communities in disaster-struck areas. Google started the Loon project in which they used ‘internet-beaming’ stratospheric balloons to create a network that could reach places and people previously unconnected to the internet (Loon, n.d.)
Also see: section 3.1.

Smart fabrics, textiles & wearables

Smart fabrics embed digital elements such as batteries, LEDs or sensors.

*Also see***: Smart Textiles / Wearables & Sensors** in section 3.3.

Metaverse

The metaverse is seen by many experts as a 3D model of the internet, a parallel place to the physical world. Humans can enter this parallel place via their 3D avatar that is used to interact with other people in the metaverse. Virtual Reality can be seen as a tool to experience the metaverse (Joshi, S. 2022).

The objective of including the metaverse as a source of data for IMPETUS, is to collect data in public rooms that are accessible within the metaverse.

Nanotechnology

Overall, Nanotechnology makes it possible to work with particles the size of a nanometre, close to the size of an atom. An objective is to create new structures, materials and devices.

Network of tools

By creating a network of the tools within the IMPETUS platform, tools can use data from sensors collected by other tools, such as the BD.

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

Pervasive AI

Objective: better supporting human activities by providing a more global and complete view of the environment.

Also see: section 3.1.

Voice-to-text Conversion

Converting voice recordings into text documents can either be done manually by a human transcriber, or by AI transpiration software. Such AI software perform speech recognition which is part of machines ability to perform Natural Language Processing. It allows to transform audio data into text format for further analysis.

Web semantics / ontologies

Objective: knowledge base for attack graph enrichment**.**

Table 5: Technologies and their expected impact on specific tools

Technology	Impacted tool	Expected positive impact on tools	Expected challenges and constraints
AI-enabled surveillance cameras	FD	On-scene video footage that can be analysed by the FD.	It changes the operations and might require new drills and exercise. Body-worn cameras tend to create a lot of new video footages that might need storage (auditing purpose) and analysis.
Bidirectional BCI	WMS	Extend the tool from detecting to e.g., steering the operator in the field to move in a certain direction, focus or steering of the attention of the operator.	Human users need to be willing to let the technology 'steer' them.
Smart fabrics, textiles & wearables	WMS	Will result in integration of the technologies in smart fabrics (input and output as well as contains and possible generate power supply).	Wearers need to agree with wearing any type of sensor (textile or wearable). Certain fabrics or adhesive materials could cause skin irritation on the wearers.
Nanotechnology (sensors)	WMS	This will reduce the challenges of wearing a (measurement) device that performs operator monitoring. It can furthermore optimise the quality of the result (increase resolution).	Occupational health risks associated with manufacturing and using nanomaterials are not yet clearly understood.
Internet for Everyone	WMS CTDR	WMS becomes independent of location. CTDR can faster monitor all the tools. A challenge that is created is the amount of data that needs to be stored and processed.	Certain companies have tried to launch IfE in different ways and have not yet succeeded. Many geographical constraints need to be overcome. It is already a costly endeavour.

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

Technology	Impacted tool	Expected positive impact on tools	Expected challenges and constraints
Semantic Web / ontologies	CTDR	Ontologies help representing a domain in a structured way. This ensure that knowledge is always available and accessible for machines. Ontologies provide structured information about vulnerabilities and countermeasures that is used for mapping which allow the enrichment of the attack graph.	
Voice-to-text conversion	SMD	With the maturity of such technologies, it becomes possible to extract text from voices coming from audio and videos files, found on blogs, YouTube and maybe even live streams.	A challenge concerning this technique is that it is incapable or less reliable when people speak with regional accents, dialects or abbreviations, or when people speak in code.
Metaverse	SMD	When the Metaverse is added as a source of data, more data can be collected and used for analyses. SMD can collect data in public rooms in the Metaverse.	A negative impact is that the line between private and public will be thinner. Accounts are needed, that can be faked or are generated by bots which will make the collected data less reliable.
Network of tools	BD	When a network of tools can be created, the BD can sent information to UAD for further analyses.	
Integration of (additional) sensors (similar to the BD sensor)	BD	Currently, an event can be predicted. Additional sensors can help to evaluate e.g., which people will be affected by the bacteria and send help to a specific location. Additional sensors can help understand the microbiology of the air in a different room under different conditions, and it further allows the tool to cover more/ specific location.	If more sensors are used, more maintenance to these sensors is required, and more data will be gathered by the sensors. This might require more storage and processing capacity.
Pervasive AI	UAD	The advantage is that a more complete view of the environment could contribute to a more complete or accurate SA.	It will require new hardware and software, and new meta learning techniques.
(Extensive use of) Big Data technologies	UAD	Enables correlation of the outcomes of smart cities services such as the ones of IMPETUS tools extracting advanced knowledge and providing decision support for users.	

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

Technology	Impacted tool	Expected positive impact on tools	Expected challenges and constraints
Counter-person sensors	EO	Sensors that count people are crucial for the use of the EO. An indirect way of counting people, is tracking the number of mobile devices within a specific area at a given time. This holds especially for contexts not equipped with counting person infrastructure. By knowing the precise number of people within an area it is possible to better estimate the flow (and the risks) during egress scenarios, thus it is possible to further optimize the emergency response.	For a timely response, the data must be in real-time. Counter person sensors must be linked to the infrastructure, sending data to the platform. A historical data set is essential to provide a baseline for evaluations expressed in terms of average daily people circulating within the public space. These evaluations must be performed directly by the operator offline. It would be positive for the tool to provide artificial intelligence for periodic assessments in the future. When counting WIFI signals, it is important to adhere to the privacy rules and guidelines.

3.5 Identified technologies expected to be used in adversarial ways

Besides creating awareness of technologies that can be beneficial for the IMPETUS platform, it is worth mentioning technologies that are expected to be used to purposefully undermine or negatively impact the performance of the IMPETUS solution. Technologies used in adversarial ways or for criminal intent, such as breach and attack purposes, will also evolve and become more advanced in the future. At the same time as new technologies evolve to enhance the IMPETUS solution's efficiency, one can envision that both cyber-attacks and physical manipulations of data will evolve and pose challenges to the use of the already existing technologies and the future technologies.

Several tools developed during the IMPETUS project are helpful in certain stages of a cyber-attack. The CTI exposes early signs of cyber risks to an organization's network and the CTDR detects cyber vulnerabilities in IT systems and makes countermeasure suggestions. However, not all types of attacks mentioned in this chapter can be detected by these tools. Other steps that can be taken as countermeasure for cyber-attacks is the training and education of the users. Practices and guidelines for proper counteracting could also be developed and put in place.

Being aware of the evolutions taking place regarding technologies for adversarial use, helps to build resilience to these technologies when they are deployed towards the IMPETUS solution. Identifying the threat landscapes for the tools will also help raise awareness for the users of the tools.

In deliverable 5.2 Initial mechanisms to preserve privacy in the secure smart city, further technologies that negatively impact the use of AI/ML are mentioned and described as risks (backdoor injection, model theft, inference attacks). Table 6 summarizes the impact on IMPETUS of the technologies described in this section.

Data poisoning

Data poisoning has two main categories. The first are attacks to the availability of an algorithm. It involves attackers introduce as many false data into a dataset as possible. The result will be that the machine learning algorithm will be completely inaccurate. The other category involves more sophisticated attacks against the integrity of an algorithm. It introduces an unnoticeable backdoor to the database that lets attacker control the database. If Machine Learning algorithm learns from this corrupted database, it will draw unintended or harmful conclusions (Thorpe, 2022).

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

Manipulating the data that is entering the model to be labelled can also create false alarms or misses. Adding a single pixel, transforming and image or adding noise are effective methods in significantly reducing the prediction accuracy of pre-established AI models and algorithms (Aynaci & Köse, 2021).

DDoS

"*Distributed Denial of Service (DDoS) targets system and data availability and is a significant threat in the cyber landscape. Attacks occur when users of a system or service are not able to access relevant information, services or other resources. This can be accomplished by exhausting the service or overloading the component of the network infrastructure*." (Lella, I. (Ed.) et.al, 2021)

Physical manipulation of data

Data can also be manipulated without forcing unlawful access to a database. Physical manipulation of sensor measurements for example. A classic example is the use of infrared (IR) LED on a television remote. Another way of attacking a sensor channel is by using electromagnetic interference (EMI) to create voltages on a sensor circuit. Such manipulation can seriously alter electrocardiogram (ECG) data and safe usage of other cardiac implantable electrical devices (Brown et al. 2016).

Ransomware

Ransomware is a variant of malware and encrypts data with a key unknown to the data owner. The goal of a ransomware attack is mostly financial. The last years the attacks become more focussed on targets that can pay higher ransom money (Nationaal Cyber Security Centrum NCSC, 2020). It is also expected by some, that ransomware will become more automated using AI and machine learning. This could automate and personalize attacks which will broaden their target groups again. Since the ransomware attackers have earned quite some money in the last years, it is becoming more plausible for them to hire AI and ML experts if they can offer more money than traditional companies can (Alspach, 2022).

Table 6: Technologies expected to be used in adversarial ways

Technology	Expected impact on IMPETUS	Possible countermeasures
Data poisoning	IMPETUS tools may encounter more false alarms or misses. Events could also be misinterpreted or the severity might be incorrectly detected. UAD is affected strongly. When data is poisoned, the tool could see events that are not happening in real life, producing false alarms. The quality of the tool therefore decreases.	Train and educate users to quickly detect data poisoning. Identify threat landscapes.
DDoS	If a DDoS attack is launched against the IMPETUS platform, no data transfer can take place. Sensor data might not reach the tools for analysis, or the analysed data resulting in a detection might not reach the SOC operator. This also affects data collected or created after the attack took place because, if the attack affects files used by the database server, the new data cannot be saved.	Train and educate users to quickly detect DDoS. Identify threat landscapes. Deployment of CTDR and CTI.
Physical manipulation of data	Electromagnetic interference (EMI) can affect data from e.g., operator monitoring tools. Wrongly classified operator states can affect operational processes in a negative way.	Train and educate users to quickly detect physical intrusions/manipulations. Identify threat landscapes.

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

Technology	Expected impact on IMPETUS	Possible countermeasures
Ransomware	If ransomware enters the IMPETUS platform, the data cannot be accessed anymore. UAD will be affected strongly when encountered with ransomware which will reduce the quality of the tool output. Since the IMPETUS platform and corresponding tools are built on data, ransomware attack can have a huge impact on the platform functionalities. However, once in production, a proper recovery plan must be implemented to counteract this type of attacks.	Train and educate users to quickly detect ransomware. Identify threat landscapes. Deployment of CTDR and CTI.

3.6 Summary

This chapter described the identified trending technologies that are expected to have an impact on IMPETUS, whether it is on the whole platform, certain platform capabilities, operational processes or specific tools within the platform. The expected positive impact is described together with the foreseen negative impacts including constraints when implementing the technology into the platform, or broader negative sides such as the added need for training the user.

For further development and improvement of the IMPETUS platform, the technologies from section 3.1 and 3.2 are most relevant. The technologies mentioned there are expected to have direct impact on the platform. If the expected positive impact outweighs the constraints or negative impact, actively adopting the technologies might be the logical next step in development.

The technologies described in 3.3 are relevant for operational processes concerning smart cities and therefore indirectly impact the IMPETUS platform. They might not need to be implemented into the IMPETUS platform to have a positive effect on the operations. The technologies described in section 3.4 are foreseen to impact specific tools. Their impact will also be indirect to the IMPETUS platform and only if the platform incorporates the specific tool. If that happens, the IMPETUS platform will automatically be impacted as well. Furthermore, contact between the technologies in 3.5 and the IMPETUS platform should be actively avoided because their aim is to purposefully oppose the IMPETUS processes.

This chapter has provided the user with a number of technologies to create awareness about opportunities for further development but also awareness of possible threats. The next chapter focusses on other important aspects of trending technologies that should be kept in mind while developing the IMPETUS platform or future versions thereof.

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

4 Other expected impacts

This chapter describes impacts that can be expected from the future technological evolutions on the operational processes and ethical and legal aspects. Other impacts that can be expected and are described in this chapter are impacts from societal perspective on the IMPETUS platform and vice versa.

4.1 Impacts concerning ethical and legal aspects

The previously described technologies are likely to enhance the capacity of personal data collection and analysis. For that reason, it is important to note that all current legislation must be fully adhered to by all developers and deployers, not only within the context of the IMPETUS platform, but also for advanced versions that incorporate previously described technologies. General ethical concerns regarding the technology's invasion into personal space and personal data have been described within the IMPETUS Deliverable 1.2. The IMPETUS Deliverable 5.1 and Deliverable 5.3 are focused on the current technologies and current/upcoming legal framework regarding the protection of personal data. Having in mind the upcoming European Union's Act of Artificial Intelligence (summarized in Deliverable 5.3), as each new technology is implemented into the IMPETUS Platform, it will be necessary to assess the application of the noted AI Act on each particular technological tool. Albeit touched upon in Deliverable 5.3, it is worthy to highlight that the new AI Act will be based on risk approach, meaning that all technological tools representing a high threat to the protection of personal data will be allowed to be deployed only in very limited and restrictive purposes. This is of particular importance for the public security sector where the Law Enforcement bodies will be the only actors allowed to use certain technologies (i.e., facial recognition in real time), and only under very particular set of conditions that must be satisfied. For more information, please refer to the previously noted IMPETUS Deliverables.

4.2 Societal developments and impact

Beyond the evolutions and their impacts that are expected in technological domains, evolutions and impacts can also be foreseen on a societal level. Society is the main creator of the data used in the IMPETUS platform, meaning that changes in society might affect the analysis performed by the IMPETUS platform. On the other hand, technologies used by the IMPETUS platform might have an impact on society and how it behaves. Because such impacts could alter the effectiveness or performance of the IMPETUS platform, it is good to be aware of them in advance. Both directions of the dependencies between the platform and societal behaviour are described below.

4.2.1 Society affects IMPETUS

The amount and type of data produced by society can fluctuate and change over time. Where certain social media tools or technologies are used during one period of time or in one specific geographical location, their use can change over time or in different locations. After its introduction in 2013, Instagram caught up the number of users over Reddit, Twitter, and Tumblr. Similarly, since its introduction in 2017, TikTok has passed Twitter and Reddit in number of users (Ortiz-Ospina, 2019). The digital output of both social media platforms are short videos, and photographs, instead of short text. This societal evolution will impact the data used by tools in the IMPETUS platform such as the SMD tool. The SMD tool currently analyses text. If the relevant data will change to a different output format the technologies used for analysing the data has to change accordingly. An emerging technology that could be added to the analysis process is speech-to-text conversion. Such technology allows to transform spoken information in videos, blogs or even life-streams into text. The text output can then be used as input for SMD.

4.2.2 IMPETUS affects society

Another impact between technology and society, is that certain technologies trigger societal concerns. Even after CCTV proving to be effective in reducing crime and tracking down terrorists, society is still concerned about the violation of personal privacy by these systems and their cost-effectiveness. More recent concerns raised by

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

European watchdogs, is the use of facial recognition systems. They ask for a global ban of the technology in publicly accessible areas (Weiss, 2021).

Besides concerns of the general public and societal watchdogs, another reaction towards tools and techniques that fight crime, is the adaptation of criminal behaviour. As Europol stated in their SOCTA (Europol, 2021):

"A key characteristic of criminal networks, once more confirmed by the pandemic, is their agility in adapting to and capitalising on changes in the environment in which they operate. Obstacles become criminal opportunities and may be as simple as adapting the narrative of a known modus operandi".

Even after adopting an IMPETUS platform in a smart city environment, evolutions to the platform are necessary to stay effective in an environment where criminals proved to be agile and resourceful in overcoming new safety measures. An example could be that criminals learn about weapon detection technologies and will start to camouflage their weapon to avoid detection. As addressed in 3.5, awareness of the currently used technologies for criminal purposes is already a step in overcoming the new threats.

4.3 Summary

This section describes different ways in which society, the IMPETUS tools and the IMPETUS platform can interact and affect each other.

As the IMPETUS platform evolves, it will likely enhance the capacity of personal data collection and analysis. Adhering to all current and coming legislation is therefore of utmost importance. Being aware of societal evolutions will increase the adaptability of the IMPETUS platform to evolve along with the societal evolutions and will keep the platform effective in future scenarios.

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

5 Design fiction for future technologies

With the help of Design Fiction, the impact of the trending technologies described in D6.5 on the operators using the IMPETUS platform in the future, is demonstrated. The story told in this chapter is based on the scenarios that were used during the validation of the IMPETUS solution during the live exercises. The IMPETUS platform is described as a diegetic object (Kirby, D. 2010), which means the object is created in the fictional world through dialogue, character interactions and the narrative. In this chapter, the platform is a 'real' object that functions, and people are using it. This chapter enables us to demonstrate the need and viability of the object.

The story takes place in the year 2050 and uses a wide view on the world. A graphical timeline of the story is shown in Figure 2. It not only includes the user and the IMPETUS platform but takes a social and political context into account. We are not limited by the currently used technologies but use the identified technologies to examine a somewhat distant future (Bell. F. et.al., 2013). We created a story around the IMPETUS platform that is set into the future, while it remains unclear if this future will happen. However, this future narrative has the potential to create interesting discussions among tool providers, technological experts, users of the platform. With an exponential increase of technological advances combined with the changing social and cultural climate in cities, it is becoming increasingly important to keep asking the important questions about technologies, the IMPETUS platform and our future.

5.1 Current scenario

5.1.1 Background

During the Covid-19 pandemic, the satisfaction towards local governments has decreased drastically amongst some groups. As there has been a period with fewer restrictions, these groups are very angry with the fact that restrictions are once again going to be imposed. This leads to the planning of a demonstration outside City Hall during the political assembly that will discuss and implement the new restrictions.

5.1.2 The night before

On the evening of Wednesday 17th August, the CTI-tool in the City Hall SOC detects a cyber threat towards its infrastructure. Later that night, the SMD-tool detects plans of a demonstration at 11:00 the next day. Following up on this detection, City Hall runs EO-evacuation scenarios, and alerts the municipality coordination centre and the Police.

5.1.3 Demonstration day

When the protesters arrive outside City Hall, police have already set up security with City Hall. The demonstration becomes gradually more aggressive and violent, accumulating in a weapon detection after some time. A bacterial attack threat is registered with City Hall through a phone call, which rises both stress and concerns. Approximately an hour after the demonstration was started, a bacterial attack detection is registered, alongside with the fire alarm going off. This calls for an evacuation of City Hall, and the need to end and disperse the demonstration. After the evacuation of City Hall, employees are evacuated to a next-of-kin-centre in the nearby neighbourhood of St. Hanshaugen for registration and support.

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

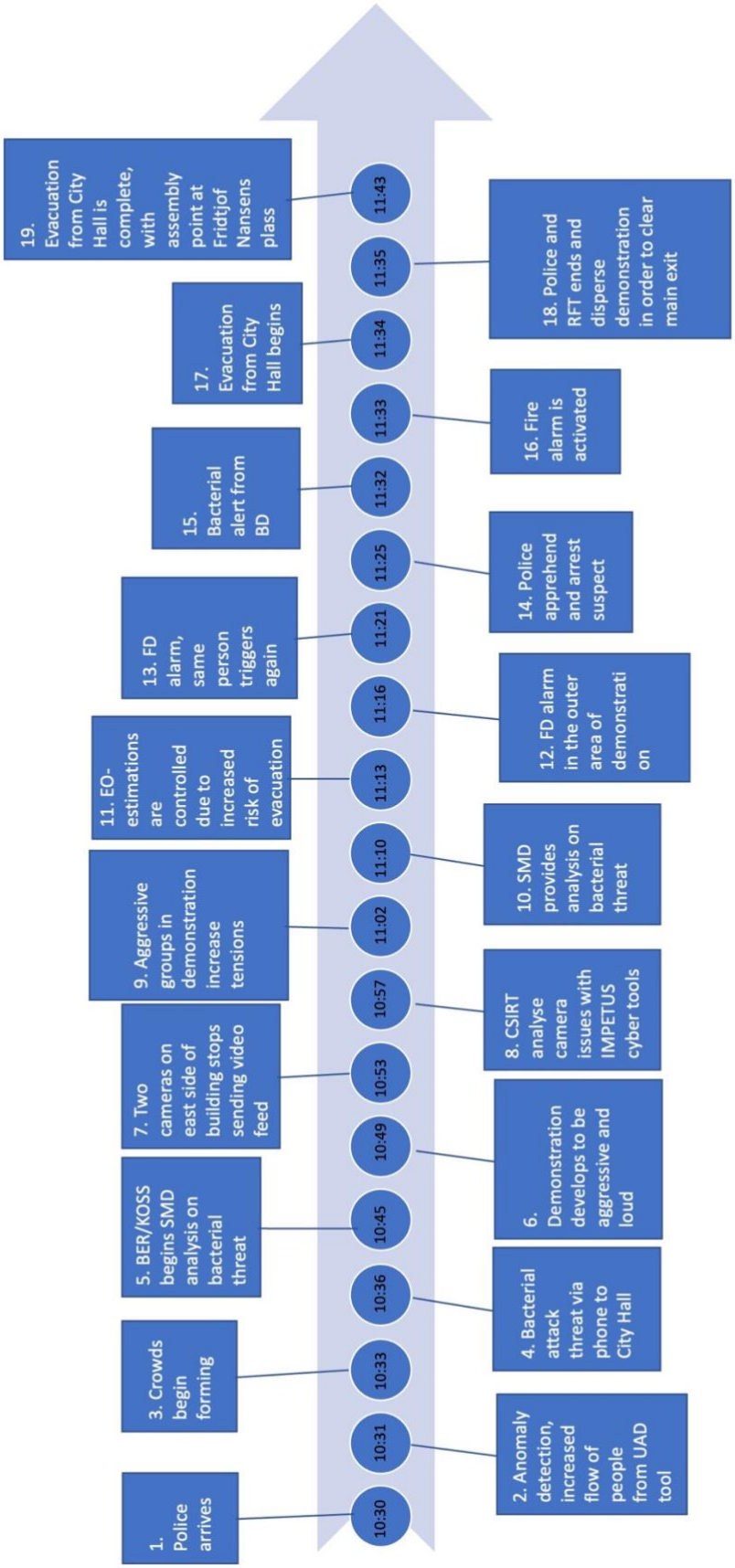


Figure 2. Graphical timeline of the scenario used during the live exercise in Oslo.

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

5.2 Future design fiction story

This scenario takes place in the year 2050 and describes the use of the IMPETUS platform in its future context. It describes the life of the main character David. Several technologies from the previous chapters are mentioned in the story. They are annotated with a colour highlight that corresponds to a category of impact. In the text box, a legend explains the annotation and the link to the highlight colours.

Main character:	David McGreen
Age:	41 years
Date:	September 2050
Profession:	Smart City Security Operations Centre Operator for the city of Oslo
Employment:	4 years and 7 months for the city of Oslo
	8 years with Norwegian Center for Information Security, Gjøvik
Education:	Master degree in Computer Science, University of Stavanger
	SOC analyst certified, CDI Norway

David is a SOC operator for the city of Oslo. He is the senior operator, leading a team of four other junior SOC operators. He is responsible for implementation of the technology within their Smart City Safety Platform (SCSP) called IMPETUS, overseeing day to day operations and being the main liaison during large events in the city. Within this story, every technology that is mentioned contribute as direct primary functions of the platform or via an interface connected to the functionality of the platform.

In the design fiction story the future technologies are tagged. The tagging shows what aspects future technologies have an impact on. The categories are tagged based on the results from the previous chapters. See below for the legend.

Platform as a whole
Adversarial use
Data transfer capability
Data processing capability
Security and privacy capability
Operational processes
Specific tool

The last three weeks, David McGreen has been working remotely. Thanks to his new VR-glasses and cloud computing services, he can do his work from home. Since the outbreak of the COVID-49 virus it is impossible to travel to his workplace. Since 2050, only service robots and people with a permit are allowed on the street. Luckily, since the new law of 2039, every employer has to enable employees to work from home.

It is expected that the new virus, with an incubation time of six weeks, will have perished within the next four weeks. David has been at home for the past five weeks already. He has seen an increase in cyber-attacks on the city infrastructure. Due to the drought, people get limited access to drinking water. The drought started in July 2050 and has a grip on the city for the last two months now and civil unrest is rising. The forbidden hacker group 'Waterfront' has been trying to disrupt the water distribution service more intensely in the past week. Another concern from the past few weeks is that the smart city AI cloud services have been warning about an attack on both the digital and physical infrastructures in the city.

David is planning to travel to the office more frequently to have better access to the services of the city. He has a permit from his employer for each day. Tomorrow, he is planning to travel there. One of the AI cloud services expects a forbidden digital demonstration in the Meta-verse at the main city building, this is also the building where David works. David has been using the traceability and eXplainable AI feature of the AI cloud service to identify how the service came to this conclusion. The service concluded this based on the big data set that is collected about all the inhabitants of the city, mapped with modelled behaviour data of larger crowds and the trend in the current political climate and increased restrictions on freedom of movement of individuals. He will therefore travel early tomorrow using the self-driving service car of the city. This is safer at the moment because these cars are never stopped and searched by the security service robots.

David disconnects his mobile phone from his workstation at home. He has done enough for today and cleared all the security alerts from the security system. He wants to get some sleep, but first has to set the **WMS** alert

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

threshold to adaptive. The adaptive setting means that based on his personal mental state and sleep stage at the moment of the alert, the system determines if he should be woken up by an alert this night. If he is too tired or overloaded to accurately respond to a security alert, the automated system will take preventive actions itself, unless human intervention is definitively needed. If so, the alert will be diverted to one of his colleagues who is in a better state. He still finds it difficult to adapt to this new system, but since a few weeks, he notices he is better rested during the nights he set the threshold, even when an alert wakes him up. He feels rested and his performance during the daytime has increased.

As David moves from his workroom, the lights and systems are automatically set to hibernation mode or turned off. The moment he steps in bed he receives a message on his mobile phone from the city's broadcasting messaging service. The message says: “An attack on the energy network has been detected and power services in your neighbourhood might be affected”. For David this is no problem, his apartment building is self-reliant, but looking outside, he sees that some of the surrounding buildings are completely dark.

With the current temperatures during the summer, the buildings are not cooled. This could even affect human lives with the currently rising temperatures. “Better hope they get the energy back up and running before tomorrow, they expect a maximum temperature of 41 degrees”, David thinks. Even the smart lighting outside appears to be off, though these are supposed to be solar-powered and should be used in cases like these; guiding people to a safe place or at least give some light when energy is limited. With a sigh, he steps into bed; hopefully this is no forecast for tomorrow.

David is rudely awakened. His phone is buzzing. He looks at the screen. It is 04:41. The message reads: “Increased threat level for bacterial attack during illegal crowd protest near the city main building, probability is high. Advised evasive actions, based on simulation data, are: closing of access to the city main building and alerting the police force for additional back-up. Staff the main city building.” This is the first time during the COVID-49 stage that this message has been sent by the AI cloud service.

David gets up and dressed as quickly as he can. The pervasive AI has already ordered the shuttle service and sends a notification to David’s phone. It will be there in 7 minutes. David exits his apartment and takes the stairs. Trust in the building’s power supply is high, but getting stuck in the elevator today would be terrible. When he arrives downstairs, the shuttle is already there. The authentication process to enter the car is really good; it allows David to enter, and nobody else. He uses his City Identity card which contains a lot of personal data and the facial recognition in the car. These technologies enable him to use additional services in the city, among which, the free shuttle service.

In the shuttle service, a generic workstation is available. He can connect his identity card and his phone to this workstation and work during his travel to the city centre, where the city main building is located. Even the connections to cities 8K video feeds can be accessed on this workstation. The latest version of the 5G rollout is great; it supports a better bandwidth and latency compared to when he started at the city of Oslo in 2046.

Clicking one of the video feeds is instantaneous, there is no lag whatsoever. Before David can use the workstation in the shuttle, he has to identify himself, wearing the smart clothing, provided by the city, speeds up the process. His data is stored in the fabrics and they measure his personal physical characteristics; his breathing rate and depth, electrodermal activity, heart rate and heart rate variability. Using the City Identity card and his personalised model, he is identified, and the data of his destination is loaded in the shuttle. His location is shared with the police, because of the current curfew that is in effect. The vehicle won’t be stopped this morning. His estimated travel time is just 31 minutes, clearly shorter than without a curfew. Even at this hour, it would normally take him around one hour to get to the city centre.

During his travel, he uses the workstation on board. When diving into the details, regarding the attack on the water infrastructure, he sees suspicious data being transferred. The data representing persons of various ages are identified by the AI as possible members of the ‘Waterfront’ hacker group. Ages above eighty and children below the age of six. Very unlikely, David thinks, this might be a case where the hacker group somehow got access to one of the databases. David checks the Cyber Threat Detection and Response to find out what the possibilities of a hack could be. CTDR suggests that it could be one of the less secure databases of Internet for Everyone, that enables people in rural areas to connect to internet as well. These connections are less secure and shared via a local mesh network to optimise the connection. People, who share personal data on these types of networks are often the victim of identity fraud. But it appears, that the hacker group used this data to poison the

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

data of a routing service in one of the main infrastructure lines for the water provisioning. These names pop-up as identified users who are using more water in the city, while they are not even living in the city!

David checks if the Urban Anomaly Detector has identified these anomalies. The tool has them listed but due to specific threshold for sending alerts, David or one of his colleagues did not receive any notification. What will happen is that the city will charge these individuals a fine and they will be shut-off from the central water supply for three months, while having done nothing wrong. David notifies the accounting department of the cyber-attack and that the names appear to be just regular people without criminal records. He asks them to have a look at the distributed ledgers of the cities power and water supply. In there, they can retrace if someone is changing names of the users of the water.

David is one minute away from the city main building, when he gets a new alert. It states: "Based on current social media conversations on the social media platform Meta-verse we expect an imminent bacterial attack in the city centre." This is the new speech-to-text service that has been implemented, this service can even transcribe real time video on Meta-verse and translate it in twenty-seven different languages. They validated the tool a week ago. When David thinks about it, he wonders 'is this alert reliable or does the service still needs more calibration? If this is legit, this is serious.' After a quick glance, David thinks it is for real. He arrives at the city centre and quickly scans the Firearm Detection notification list to see if he missed anything. The tool has not detected any weapons in the area, so David runs towards the entrance.

He already sees security service drones flying overhead. They appear to have identified him correctly because they swivelled off. Running towards the city main building might not have been such a good idea, it could quickly have been identified as a threat. In his earpiece, he hears that the main entrance of the building is closed. He is guided by haptic feedback in his clothes to a security entrance at the side of the building. This works better than looking at his phone for directions. He remembers the security entrance from his safety training, but with the current pressure he would have run past it, if not for the haptic feedback giving him force-feedback on his chest. He immediately stops. Guided by small vibrations on his left hip, he looks to the left. He sees the door and runs towards it. It sways open and closes directly behind him.

When David enters the SOC room, his workstation already shows the latest state of the bacterial threat alert. The source is a conversation in a public VR Meta-verse room, where unidentified individuals with spoofed accounts are talking about releasing a specific agent in the city centre. He sends the data off to the police unit. David is wearing his official uniform. That uniform has a Brain-Computer interface embedded in it which includes EEG to read his brainwaves. After a few minutes in the SOC room the BCI prompts David that his Mental Workload is abnormally high and suggests he should calm down. David takes a deep breath, re-orients himself for a moment, and then replies to the BCI's AI, via voice command, that all is well, and he is in control and fully capable to perform his duties. The BCI AI acknowledges, and lets him continue. David really appreciates the fact that after the upgrade the processing of his EEG data is done on the device itself using his personalised AI.

He sees on CCTV from one of the cameras around the building, that additional UAVs and additional Unmanned Surface Vehicles (USVs) enter the square in front of the building. While David looks at the screen, multiple cameras turn off. They are instantly replaced by the camera feed from the UAVs and USVs on the square. David checks the cameras' data traffic, using the distributed ledgers. They appear to be offline for maintenance, while no maintenance was planned, especially not during an expected demonstration! It appears, that someone has physically manipulated the maintenance data. This person must have known the cameras turn off automatically when maintenance is planned. David assigns the restore actions to one of the support services, as he doesn't have the time now to fix it himself. These services are also tasked with scanning for potential cyber vulnerabilities. This includes scanning for spyware or wipewear like the infamous NotPetya or any of the similar threats.

Two alerts are shown on his workstation at the same time. One of the alerts directly disappears, the other is shown on the screen. It appears to be a live call David is included in. It is a call to the emergency services and the operators have included the relevant organisations in the live call to listen in. An unidentified person is calling from a phone that can't be traced to a person, but is localised close to the city main building. CCTV cameras swivel to the position and two UAVs move in that direction. The person mentions that a bacterial agent has been deployed in the street behind the city centre. The UAVs that have been deployed have an outer shell with metal-based nanoparticles that are effective against pathogens from a lot of bacterial sources.

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

David's workstation suggests an action from a pre-defined protocol list. The action can be tailored and updated, based on real-time simulations, using the current location of the person, the wind velocity, and the current building plans in that area. David accepts the systems suggestion 'immediate action to evacuate the human personnel from this area and have them move towards a building up wind'. The system suggested to David that the specific building has safety precautions in their climate control system with an anti-bacterial filter. The system suggests the just renovated St. Hanshaugen has enough space.

The number of individuals on the street is limited; the system identifies 14 humans, from which 9 can be identified automatically. The other five are unidentified, but appear to be moving in the right direction of St. Hanshaugen. They have received digital instructions, using the cities broadcasting messaging service, that is also connected to David systems. A part of the city main building is evacuated as well, one of the anti-bacterial filters has failed and persons are directed out of the back of the building and directed towards the St. Hanshaugen.

City personnel that have no clothing with haptic feedback are guided via an automated system. This system calculates, after a simulation, the optimised path for the people, to get them to their destination as quickly as possible. This system avoids guiding through overcrowded areas to minimize the probability of contagion with any bacterial source. The system guides the people using smart lighting and navigation instructions based on their phone location.

Based on the voice data of the call, the police managed to identify the suspect and located where this person lives. They are on their way to arrest him. A USV has found the source of the bacterial agent. It appears to be in a small transformer station that was close to the city main building. The suspect used an analogue trigger to release the agent in the air. The USV is equipped with a sensor that can identify the main component of the agent but is not 100% certain. A sample is taken and a UAV is transporting it to the specialist unit for analysis. David advises the police to keep the city main building and the square closed for now, due to the failed bacterial filter in the building and the uncertainty of the agent in the air. There is still the digital threat of the 'Waterfront' that might impact water storage that is in the vicinity of the square.

5.3 Summary

The previous section followed David as he works as a Smart City SOC operator in a futuristic setting. This story represents the majority of aforementioned technologies from chapter 3. Presenting the technologies and their expected impacts in such a way helps the readers to envision future settings in which these technologies play a part.

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

6 Future work

So far, this document has identified different technologies and their expected positive and negative impacts on the IMPETUS platform, specific IMPETUS capabilities, operational processes and specific tools integrated in the IMPETUS platform. Furthermore, expected impact of technologies used for criminal activities and the impact of the IMPETUS platform in general on society is discussed.

This analysis focussed on technologies that are expected to be technologically mature between now and 2030, and aimed to create awareness of changing and evolving technologies. This awareness helps to:

- be aware of technological possibilities for enhancement and improvement of different IMPETUS aspects,
- be resilient when outside parties will use new technologies with criminal intent that will negatively influence the IMPETUS platform,
- foresee what kind of societal evolutions could impact the performance of the IMPETUS platform and vice versa, and
- in general, prepare for changes and adaptations in the near future.

One last category of technologies that was deemed out of scope in the previous chapters, is the category including technologies impacting IMPETUS aspects after 2030. This includes technologies that are still very immature or low on the Technology Readiness Level. They will be addressed in section 6.1.

6.1 Further down the line

Technologies that were mentioned during the collection phase but not categorized in the other categories are listed below. Their TRL is expected to be beyond 2030 and are therefore more 'futuristic' than the technologies described so far. Table 7 lists the technologies with a description or an objective, the tool they are expected to impact, and a short description of the expected impact.

Table 7: Technologies expected to not reach maturity before 2030.

Technology	Description/objective	Tool	Expected positive impact, and challenges and constraints
Quantum Computing	Although some optimistic project partners see quantum computers feasible before 2030, most do not. Quantum computing offers a new paradigm of computing which can offer next level of computation in a limited time periods which were not previously achievable. It is a rapidly-emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers (IBM, 2022). In communication security, cryptography represents the basic technique for ensuring information that is secure from the point of view of the indecipherability of messages. The number of cryptographic system vulnerabilities has increased considerably in recent years. The advent of quantum computers will undermine standard encryption systems	Whole platform	It is a good for resolving combinatorial problems. On the positive side it can enable a faster solution for logistics / routing problems which are good for route optimization for delivery companies and bad for cyber security. As much of the cyber security relies on difficulty of prime factor calculation in number theory. Quantum may adversely impact IMPETUS as much of the data that moves from sensors to data storage would be vulnerable at city SOCs.

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

	such as the widely used RSA public-key cryptosystem . It is therefore of fundamental importance to study post-quantum algorithms that are robust with respect to technologies that are likely to be available in a few years.		
Holographs	Provides a new way to visualise objects or data via head mounted displays.	WMS/ Platform	Expected to impact the way of communication. New way to present output information to the operator or supervisor.
Artificial brain	An artificial brain that works as a human brain.	WMS	Expected impact on the preparation of the WMS. Can be used for testing purposes.
Artificial neurons on a chip	Can be described as a brain on a chip.	WMS	Will redesign how operator parameter is modelled.
HMT (symbiotic collaboration)	Human-Machine Teaming in this case is defined as actual symbiotic collaboration between human and machine. Its final shape consists of combined decision making where the human and machine, support each other on an equal level.	Platform	Expected to mainly impact on the operational level. End-users of IMPETUS will seamlessly work with the machine. Human and machine understand each other and know when to support the other party. This will result in a trustworthy and intuitive collaboration, meaning the HMT system can work as effectively and efficiently as possible. For further details on this topic please refer to D6.1 Initial concepts of operations.

6.2 Next steps

After reading this deliverable, the reader is expected to have awareness of future technologies that are expected to impact IMPETUS and maybe even be aware what kind of other technologies could be meaningful in the near future. Awareness itself, however, does not create 100 % resilience. Developers, planners and executioners active in all domains related to the IMPETUS platform and processes need to stay vigilant for evolutions for which appropriate adaptations in our platform, tools or operational processes need to be made.

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

7 References

5G, accessed July 2022, https://digital-strategy.ec.europa.eu/en/policies/5g

Alspach, K. (16 May, 2022). Ransomware is already out of control. AI-powered ransomware could be 'terrifying.' Protocol. https://www.protocol.com/enterprise/ai-ml-ransomware-cyberattacks-automation

Arregui-Vicomtech, H. (2021). How can AR be used to improve first responders operations: an overview.

Ayamga, M., Akaba, S., & Nyaaba, A. A. (2021). Multifaceted applicability of drones: A review. Technological Forecasting and Social Change, 167, 120677.

Aynaci, Emsal & Köse, Utku. (2021). Manipulation of Artificial Intelligence in Image Based Data: Adversarial Examples Techniques. 6. 8-17.

Bell, F., Fletcher, G., Greenhill, A., Griffiths, M. and McLean, R. (2013). Science fiction prototypes: Visionary technology narratives between futures.

Boi, F., Moraitis, T., De Feo, V., Diotalevi, F., Bartolozzi, C., Indiveri, G., & Vato, A. (2016). A bidirectional brain-machine interface featuring a neuromorphic hardware decoder. Frontiers in neuroscience, 10, 563.

Brown, N., Patel, N., Plenefisch, P., Moghimi, A., Eisenbarth, T., Shue, C., Venkatasubramanian, K. in 25th Usenix Security Symposium, Austin, TX, 2016. Poster: SCREAM: sensory channel remote execution attack methods (Usenix AssociationBerkeley, 2016).

CISCO. "What is Network as a Service?". Retrieved on 2022-07-12. https://www.cisco.com/c/en/us/solutions/enterprise-networks/network-as-service-naas.html

CISCO2. "How 5G Will Make the Network-as-a-Service (NaaS) Model a Reality". Retrieved on 2022-07-18. https://blogs.cisco.com/sp/how-5g-will-make-the-network-as-a-service-naas-model-a-reality

Cloud computing definition, NIST Computer Security Resource Center, SP 800-145, September 2011, https://csrc.nist.gov/publications/details/sp/800-145/final

Distributed ledger technology: beyond block chain (report). Government Office for Science (UK). January 2016. Retreived 11 july 2022.

EASA. European Union Aviation Safety Agency. Introduction of a regulatory framework for the operation of unmanned aircraft systems and for urban air mobility in the European Union aviation system. RMT 0230. 2022-04-22. https://www.easa.europa.eu/downloads/126656/en

Europol (2021), European Union serious and organised crime threat assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, Publications Office of the European Union, Luxembourg.

Factsheet Ransomware, Nationaal Cyber Security Centrum NCSC, 2020. Accessed august 2022 from https://www.ncsc.nl/onderwerpen/ransomware/documenten/factsheets/2020/juni/30/factsheet-ransomware

Gartner. "Gartner Trend insights report 2018" from the original on 2020-12-18. Retrieved on 2022-07-12. https://emtemp.gcom.cloud/ngw/globalassets/en/doc/documents/3889058-the-edge-completes-the-cloud-a-gartner-trend-insight-report.pdf

Goel, V., Varshney, R., Parashar S, Ali, S., Singh, P. (2022). Laser Based Smart Security Apparatus Using Arduino. International Journal for Research in Applied Science & Engineering Technology (IJRASET). Volume 10 (March 2022). DOI: https://doi.org/10.22214/ijraset.2022.40986

Gohari, A., Ahmad, A., B., Rahim, R.B.A, Supa'at, A.S.M, Razak, S.A., Gismalla, M.S.M.G. (2022). Involvement of Surveillance Drones in Smart Cities: A Systematic Review. IEEE Access, Volume 10. DOI: 10.1109/ACCESS.2022.3177904

How people counter sensors work: a tech comparison (n.d.). Terabee. Retrieved November, 17, 2022, from https://www.terabee.com/how-people-counter-sensors-work-a-tech-comparison/

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

IMPETUS (2022, October 13). Practitioner's Guide on OPERATIONS; Operational motivation for using IMPETUS. https://impetus-pg.atlassian.net/wiki/spaces/IMPETUS/overview

Joshi, S., 2022. What Is the Metaverse? An Explanation for People Who Don't Get It. Vice.com

Katikala, S. (2014). Google project loon. InSight: Rivier Academic Journal, 10(2), 1-6.

Kirby, D. (2010) 'The Future is Now: Diegetic Prototypes and the Role of Popular Films in Generating Real-world Technological Development' Social Studies of Science

Lella, I.(Ed.), Theocharidou, M.(Ed.), Tsekmezoglou, E.(Ed.) & Malatras, A.(Ed.) (2021). ENISA Threat Landscape 2021.

Loon, (n.d.) - Expanding internet connectivity with stratospheric balloons - https://x.company/projects/loon/

Miraz, M. H., Ali, M., Excell, P. S., & Picking, R. (2015). A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT). 2015 Internet Technologies and Applications (ITA), 219-224.

Morales-Herrera, R., Fernández-Caballero, A., Somolinos, J. A., & Sira-Ramírez, H. (2017). Integration of sensors in control and automation systems. *Journal of Sensors*, *2017*.

oneM2M (n.d.), One M2M, the IoT standard. https://www.onem2m.org/

Ortiz-Ospina, E., 2019. The rise of social media. Our world in data, September 18, 2019. https://ourworldindata.org/rise-of-social-media

Pothrat, Xavier (CS), 2020. D8.4 Market analysis report v1 Work Package: WP8 - Dissemination, Impact Creation and Exploitation Plan Lead partner: CS GROUP (CS).

Sikder, A. K., Acar, A., Aksu, H., Uluagac, A. S., Akkaya, K., & Conti, M. (2018, January). IoT-enabled smart lighting systems for smart cities. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 639-645). IEEE.

Thorpe, J. 2022. Exclusive: What is data poisoning and why should we be concerned? International security journal.

Vattapparamban, E., Güvenç, I., Yurekli, A. I., Akkaya, K., Uluağaç, S. (2016). Drones for smart cities: Issues in cybersecurity, privacy, and public safety. *In 2016 International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp.216-221). IEEE. DOI:10.1109/IWCMC.2016.7577060

Vodák J, Šulyová D, Kubina M. Advanced Technologies and Their Use in Smart City Management. Sustainability. 2021; 13(10):5746. https://doi.org/10.3390/su13105746.

Weiss, E., 2021. European Watchdogs Push for Stricter Facial Recognition Ban, June 21, 2021. https://findbiometrics.com/european-watchdogs-push-stricter-facial-recognition-ban-062103/

Zangelin, K.G. (2020), CEF Context BrokerT01 - Update of the ETSI NGSI-LD specifications Version 1.0. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EU+Standards

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

8 APPENDIX A: Miro boards from the workshops

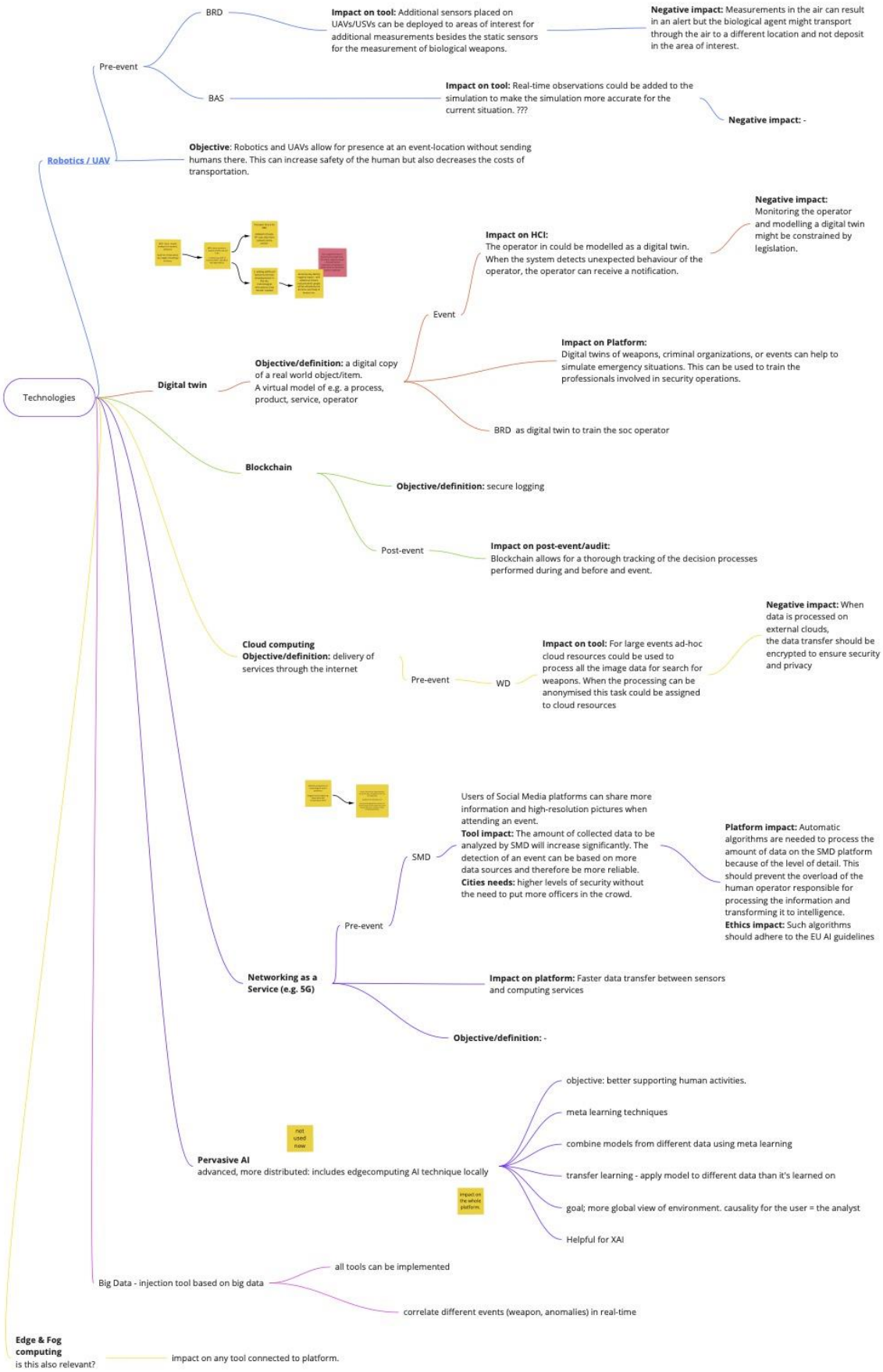
The following three pages show an export created of the Miro boards. They show the results of the brainstorm during the workshops. The results are structured in a mind map, linking specific pieces of information together. The information from the Miro boards had to be restructured to fit a more common A4 page.

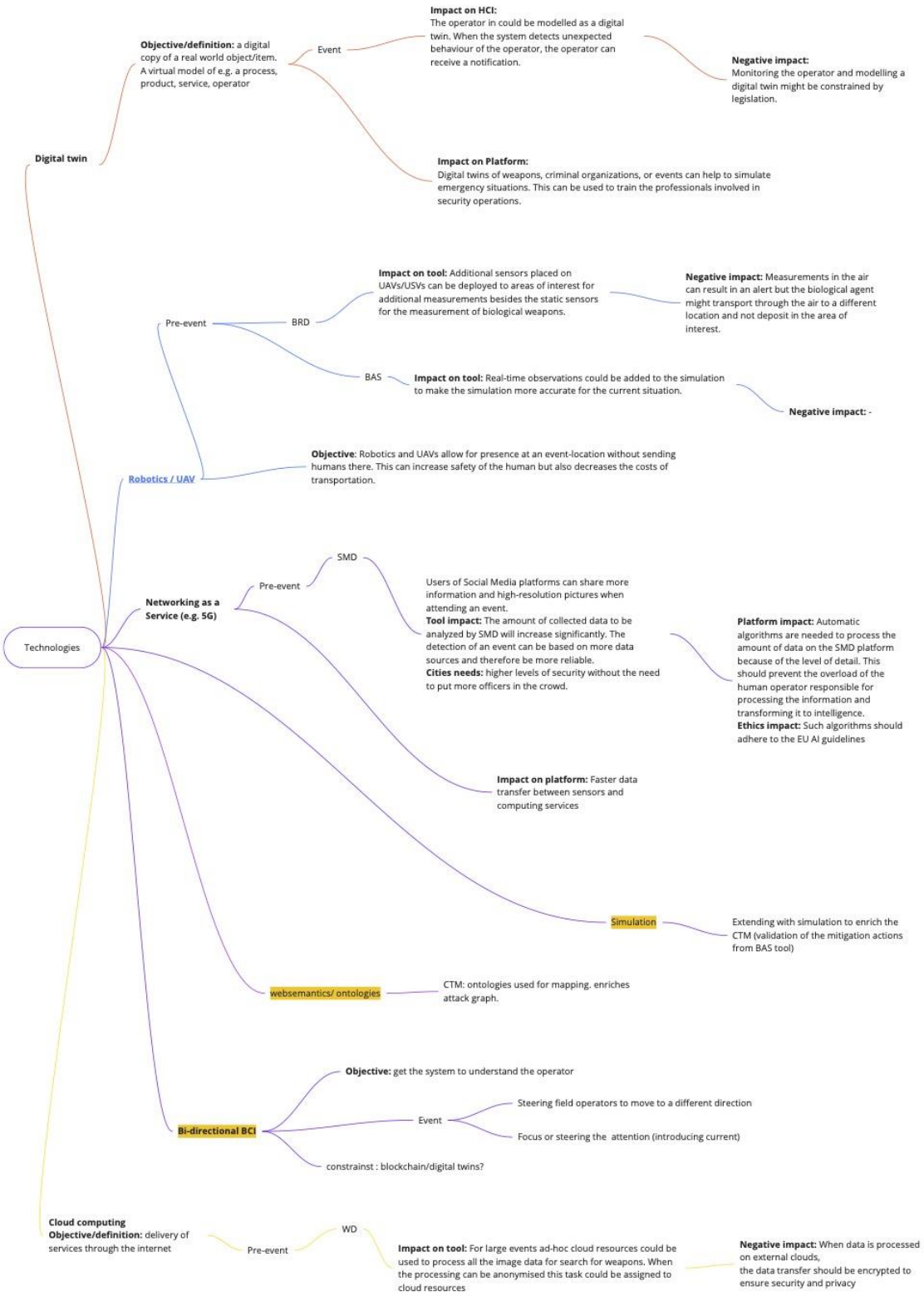
The first board is from the workshop held with tool partners working on CTRO & HCI

The second board is from the workshop held with tool partners working on BRD & PTI

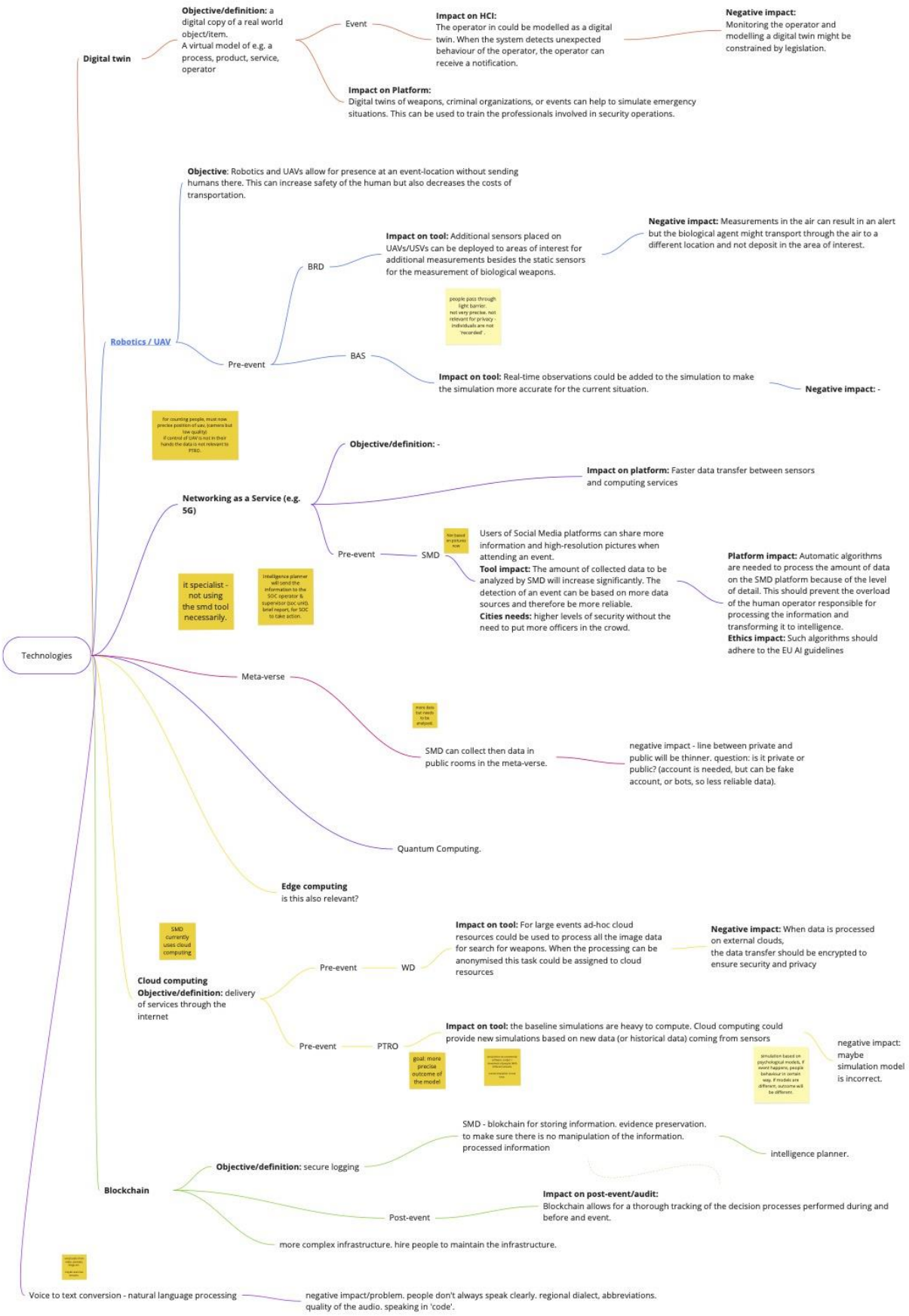
The third board is from the workshop held with tool partners working on SMD, PTRO & WD

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


Technologies
Robotics / UAV
Pre-event
BRD
Impact on tool: Additional sensors placed on UAVs/USVs can be deployed to areas of interest for additional measurements besides the static sensors for the measurement of biological weapons.
Negative impact: Measurements in the air can result in an alert but the biological agent might transport through the air to a different location and not deposit in the area of interest.
BAS
Impact on tool: Real-time observations could be added to the simulation to make the simulation more accurate for the current situation. ???
Negative impact: -
Objective: Robotics and UAVs allow for presence at an event-location without sending humans there. This can increase safety of the human but also decreases the costs of transportation.
Digital twin
Objective/definition: a digital copy of a real world object/item. A virtual model of e.g. a process, product, service, operator
Event
Impact on HCI: The operator in could be modelled as a digital twin. When the system detects unexpected behaviour of the operator, the operator can receive a notification.
Negative impact: Monitoring the operator and modelling a digital twin might be constrained by legislation.
Impact on Platform: Digital twins of weapons, criminal organizations, or events can help to simulate emergency situations. This can be used to train the professionals involved in security operations.
BRD as digital twin to train the soc operator
Blockchain
Objective/definition: secure logging
Post-event
Impact on post-event/audit: Blockchain allows for a thorough tracking of the decision processes performed during and before and event.
Cloud computing
Objective/definition: delivery of services through the internet
Pre-event
WD
Impact on tool: For large events ad-hoc cloud resources could be used to process all the image data for search for weapons. When the processing can be anonymised this task could be assigned to cloud resources
Negative impact: When data is processed on external clouds, the data transfer should be encrypted to ensure security and privacy
Networking as a Service (e.g. 5G)
Pre-event
SMD
Users of Social Media platforms can share more information and high-resolution pictures when attending an event.
Tool impact: The amount of collected data to be analyzed by SMD will increase significantly. The detection of an event can be based on more data sources and therefore be more reliable.
Cities needs: higher levels of security without the need to put more officers in the crowd.
Platform impact: Automatic algorithms are needed to process the amount of data on the SMD platform because of the level of detail. This should prevent the overload of the human operator responsible for processing the information and transforming it to intelligence.
Ethics impact: Such algorithms should adhere to the EU AI guidelines
Impact on platform: Faster data transfer between sensors and computing services
Objective/definition: -
Pervasive AI
advanced, more distributed: includes edgecomputing AI technique locally
not used now
objective: better supporting human activities.
meta learning techniques
combine models from different data using meta learning
transfer learning - apply model to different data than it's learned on
goal; more global view of environment. causality for the user = the analyst
Helpful for XAI
Big Data - injection tool based on big data
all tools can be implemented
correlate different events (weapon, anomalies) in real-time
Edge & Fog computing
is this also relevant?
impact on any tool connected to platform.



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



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

9 APPENDIX B: Technologies survey for IMPETUS partners

Survey for T6.5: Envisioning future evolutions

With this survey, I'd like to gather input for this deliverable. I need some help with describing certain technologies and envisioning impact on IMPETUS, the platform or tools.

This survey consists of 16 questions, of which some are yes/no questions. The questions are split over 4 sections:

1) technologies identified by project partners
2) technologies identified through COSSEC website analyses
3) technologies expected for adversarial use
4) review question about societal impact of certain technologies.

If you know the answers, you can easily fill-in the questionnaire within 20 minutes. If you don't know the answers, it will take you even less time because you can skip the questions!

So, please take some time to answer the questions and if you have further remarks, feel free to contact me by email: iris.cohen[@]nl.thalesgroup.com

1. What is your name and your organization?

please fill this in for proper mentioning in the author-list of the deliverable (e.g. Joe Smith (THA)).

2. Quantum computing was mentioned as a technology that could impact the whole IMPETUS platform. Please provide a short description of the technology (2, 3 sentences) and the overall benefits and constraints regarding the IMPETUS platform.

3. Will quantum computing be feasible between now and 2030?

Yes / No / Other

4. Edge computing was mentioned as a technology that could impact the IMPETUS platform. Please provide a short description of the technology and how it can impact (positive and negative) the IMPETUS platform.

5. Internet for Everyone (not Internet of Things or Everything), is he idea of connecting the last billion people on earth with a reliable internet connection. Do you foresee this technology/technique having an impact on IMPETUS?

Yes / No

6. If yes, please describe the impact you foresee of Internet for Everyone, on the IMPETUS platform, it's capabilities, operational processes or individual tools.

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

Technologies identified during COSSEC project website analyses

The technologies mentioned in this section were identified during an analysis of EU project websites klisted as possible COSSEC projects (not a have accepted). Whether or not these technologies with impact IMPETUS is the main question in this section.

7. The COSSEC (eligible) project Select 4 Cities describe Internet of Everything, to aim to connect all people, things, data and processes to the internet. Do you see any benefits of the use of Internet of Everything for IMPETUS? If yes, please provide a short description of the overall benefits and constraints regarding the IMPETUS platform, capabilities, operational processes or a specific tool.

8. The COSSEC (eligible) project 7Shield, mentions laser-fence as a technology for the detection of intruders/intrusions in a 'fenced-off' area' (using laser). Is there a tool within IMPETUS, in which such a technology COULD be implemented in the future?

Yes / No / Other

9. If yes, please provide a description of laser-fence technique and how it will impact the tool, positively or negatively (constraints needed for proper functioning)

10. The COSSEC (eligible) project Mosaicrown uses Data Sanitisation techniques to "leveraging and extending approaches for data anonymization and obfuscation, will produce sanitized versions of the underlying (structured or unstructured) data for the privacy- preserving use, sharing, and computation with other parties." see: https://mosaicrown.eu/the-project/research-work/

Do you see any benefits and constraints of the use of this technique for IMPETUS?

Yes / No

10. If yes, please provide a short description of the technique and the overall benefits and constraints regarding the IMPETUS platform, IMPETUS capabilities, operational processes or a specific tool.

11. The COSSEC (eligible) project Mosaicrown uses Data Wrapping to "design a set of techniques able to efficiently support the protection requirements expressed by the policy produced in WP3. This work will lead to the realisation of a platform for the protection of personal/sensitive/confidential information in domains involving multiple data owners." see: https://mosaicrown.eu/the-project/research-work/ Do you see any benefits of the use of such a technique for IMPETUS?

Yes / No / Other

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

12. If yes, please provide a short description of the technique and the overall benefits and constraints regarding the IMPETUS platform, IMPETUS capabilities, operational processes or a specific tool.

Technologies with adversarial use

Technologies mentioned in this section are expected to be used for criminal intent. They can seriously affect IMPETUS functionalities.

13. DDoS was mentioned as a technique that could be used against IMPETUS. Can this technique still be considered 'trending'?

Yes / No / Other

14. If yes, please describe the technique and how it is still trending.

And provide an explanation how it will (negatively) impact the IMPETUS platform, the capabilities, operational processes or individual tools.

15. Ransomware is also described as an adversarial technology. For now, the deliverable mentions that this technology will prevent us to access data. Does this also apply to accessing new data, collected or created after the attack took place?

Please provide a description on this matter and the impact on IMPETUS.

Only one more question...

16. In section 4.2 of the deliverable, the possible impact of security/observational technologies on society and societal behaviour and vice versa is described. Please read through this section and indicate whether or not you agree with the description. (Comments may also be made in the document on teams).

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

Members of the IMPETUS consortium

SINTEF	SINTEF, Strindvegen 4, Trondheim, Norway, https://www.sintef.no	Joe Gorman joe.gorman@sintef.no
Institut Mines-Télécom	Institut Mines Telecom, 19 place Marguerite Perey, 91120 Palaiseau, France, https://www.imt.fr	Joaquin Garcia-Alfaro joaquin.garcia_alfaro@telecom-sudparis.eu
UNÎMES	Université de Nimes, Rue du Docteur Georges Salan CS 13019 30021 Nîmes Cedex 1, France, https://www.unimes.fr	Axelle Cadiere axelle.cadiere@unimes.fr
cini	Consorzio Interuniversitario Nazionale per l'Informatica, Via Ariosto, 25, 00185 – Roma, Italy, https://www.consorzio-cini.it	Donato Malerba donato.malerba@uniba.it
Università degli Studi di Padova	University of Padova, Via 8 Febbraio, 2 - 35122 Padova, Italy, https://www.unipd.it	Giuseppe Maschio giuseppe.maschio@unipd.it
Entrepreneurship Development Centre for BIOTECHNOLOGY and MEDICINE	Biotehnoloogia ja Meditsiini Ettevõtluse Arendamise Sihtasutus, Tiigi 61b, 50410 Tartu, Estonia, https://biopark.ee	Sven Parkel sven@biopark.ee
SIMAVI Software Imagination & Vision	SIMAVI, Complex Victoria Park, Corp C4, Etaj 2, Șos. București – Ploiești, nr. 73 – 81, Sector 1, București, Romania, https://www.simavi.ro	Gabriel Nicola Gabriel.Nicola@simavi.ro Monica Florea Monica.Florea@simavi.ro
THALES	Thales Nederland BV, Zuidelijke Havenweg 40, 7554 RR Hengelo, Netherlands, https://www.thalesgroup.com/en/countries/europe/netherlands	Johan de Heer johan.deheer@nl.thalesgroup.com
CINEDIT INTELLIGENT VIDEO ANALYTICS	Cinedit VA GmbH, Poststrasse 21, 8634 Hombrechtikon, Switzerland, https://www.cinedit.com	Joachim Levy j@cinedit.com

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

INSIKT INTELLIGENCE	Insikt Intelligence, Calle Huelva 106, 9-4, 08020 Barcelona, Spain, https://www.insiktintelligence.com	Dana Tantu dana@insiktintelligence.com
SIXGILL	Sixgill, Derech Menachem Begin 132 Azrieli Tower, Triangle Building, 42nd Floor, Tel Aviv, 6701101, Israel, https://www.cybersixgill.com	Benjamin Preminger benjamin@cybersixgill.com Ron Shamir ron@cybersixgill.com
XM CYBER	XM Cyber, Galgalei ha-Plada St 11, Herzliya, Israel https://www.xmcyber.com	Lior Barak lior.barak@xmcyber.com Menachem Shafran menachem.shafran@xmcyber.com
Comune di Padova	City of Padova, via del Municipio, 1 - 35122 Padova Italy, https://www.padovanet.it	Enrico Fiorentin fiorentine@comune.padova.it Stefano Baraldi Baraldis@comune.padova.it
Oslo	City of Oslo, Grensen 13, 0159 Oslo, Norway, https://www.oslo.kommune.no	Osman Ibrahim osman.ibrahim@ber.oslo.kommune.no
Institut za sigurnosne politike ISP	Institute for Security Policies, Kruge 9, 10000 Zagreb, Croatia, http://insigpol.hr	Krunoslav Katic krunoslav.katic@insigpol.hr
T S I M E	International Emergency Management Society, Rue Des Deux Eglises 39, 1000 Brussels, Belgium, https://www.tiems.info	K. Harald Drager khdrager@online.no
UniSMART Fondazione Università di Padova	Unismart – Fondazione Università degli Studi di Padova, Via VIII febbraio, 2 - 35122 Padova, Italy, https://www.unismart.it	Alberto Da Re alberto.dare@unismart.it

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