Grant number: 883286
Project duration: Sep 2020 – Feb 2023
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: D10.5

Societal Impact Report

Dissemination Status: Public

Authors: Joe Gorman, Line Breivik Thompson (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 purpose of the deliverable is to predict potential societal impacts of widespread adoption of the results of the project (or similar results from other initiatives).

The primary impact will be on security, safety and ethics.

Some of the tools allow automated detection of threats that was not possible before (use of "big data" to recognise abnormal situations; automated detection of bacterial attacks); they help security staff to respond quickly and reduce/prevent negative consequences. Some tools make it more likely that threats can be detected (firearm detector, social media detection), and responses initiated.

Increased effectiveness of security staff is supported by the IMPETUS Platform (provides enhanced situational awareness), the Evacuation Optimiser, the Workload Monitoring System (measures stress levels of staff) and a set of cyber security tools. The Practitioners Guides provide staff with advice and educational materials.

Even though improvements in security are achieved, it may happen that citizens do not necessarily perceive these changes and *feel* safer; hence a good dialogue with citizens will be important.

The project can contribute to improvements in how organisations deal with ethical and privacy issues, by demonstrating feasibility and providing advice via the project's Practitioners Guides. However, there can be negative impacts as some people simply do not like surveillance. Open, two-way dialogue with citizens is needed to achieve understanding and compromise.

There may be impact in terms of gender equality. Women tend to experience insecurity in public spaces more than men do; general improvements in safety brought about by IMPETUS might reduce this gap.

Some positive financial impact is expected in terms of reductions of costs arising from the effects of crime.

Impacts in public policy can be expected in some areas, both at UN and EU levels.

In two areas of importance to society – employment and environment – we do not foresee any significant impacts.

Our overall conclusion is that IMPETUS will have significant positive societal impacts in several areas.

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.

1 About this deliverable

1.1 Intended readership/users

The deliverable is aimed at a very broad, non-technical audience: anyone with an interest in the long-term effects of Research & Innovation in wider society. We expect this would include our own consortium members, research organisations, companies involved in technological innovation, funding authorities, media/journalists, politicians, and policy makers.

1.2 Why would I want to read this deliverable?

No one can say with certainty what is going to happen in the future. But we will try our best here to make some predictions about how the work carried out in our project, and widespread adoption of the results it produced (or similar results from other initiatives), might in future influence various aspects of the society in which we live. The document will not provide you much in the way of hard facts or numbers – but we hope it can provide a better understanding of potential societal impacts in various areas.

1.3 Other deliverables that may be of interest

In some ways, this deliverable is related to *all* other deliverables in the project, in that it tries to summarise the overall long-term effect of the project as a whole – as represented by all aspects of what it produced. But we would like to draw your attention in particular to the following two deliverables:

- D6.5 *Envisioning future evolutions*
  This deliverable looks at how the IMPETUS results may develop in future, and different impacts that may have.
- D9.3 *Business cases*
  This deliverable looks at the business case for IMPETUS from the point of view of cities that might adopt project results: will the costs of adopting the results have financial benefits? In doing so, it looks at the economic costs of crime and violence and speculates about how such costs could be reduced by improvements in public safety brought about by adoption of IMPETUS solutions.

1.4 Structure of the deliverable

The deliverable has a very simple structure: it identifies key areas where societal impacts from H2020 projects might be expected, and devotes one chapter to each, analysing any potential impacts that might arise from adoption of results from IMPETUS (or from similar initiatives).

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 Safety and Security

The IMPETUS project placed a significant emphasis on safety and security throughout its duration.

There were substantial efforts made to ensure that **security requirements** relating to technology (e.g., security by design) were adhered to during project implementation.

The safety and security work conducted in the project went beyond its immediate activities **to encompass the challenges associated with the widespread adoption of technological solutions for public safety**, including **Big-Data** and **AI-based technology**. In this regard, the project outlined *principles and good practices* to be followed, to promote also a proper cyber-security hygiene among smart city users.

This chapter provides a detailed exposition of these issues.

2.1 Introduction

Ensuring the safety of citizens is arguably the most fundamental duty of government authorities in any society. Recalling that the official title of the IMPETUS project is "*Intelligent Management of Processes, Ethics and Technology for Urban Safety*" we consider that the core societal impact of the project is on *safety*.

We have chosen to also include the word "security" in the title of this chapter. There is sometimes confusion about the difference in meaning between the words "safety" and "security". Indeed, in some European languages (such as Norwegian) there is only one word. The words are essentially two sides of the same coin. Definitions vary, but we choose the following:

Safety	The state of being free from danger or risk
Security	Measures taken to prevent or limit danger and risk

The reason for making these distinctions is that we consider that IMPETUS will have societal impacts on *both* safety *and* security.

This chapter describes the societal impact on safety and security by illustrating with specific results from IMPETUS. But we must remember that IMPETUS is not the only show in town: other projects and activities are developing technologies and approaches along the same lines as IMPETUS. And others will surely emerge in future. By having already shown the feasibility of the approach in the course of the project, IMPETUS will serve to encourage further development and adoption of the type of technology developed and demonstrated in the project. We therefore wish to strongly emphasise that the potential societal impact of IMPETUS will be much wider than just through use of specific IMPETUS results; the illustrations shown here with specific IMPETUS results are just a starting point.

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 Improvements in safety and security

2.2.1 New ways to detect possible threats

The IMPETUS **Urban anomaly detector** continuously monitors data gathered from multiple city sensors over long time periods and uses AI/Big Data techniques to create a detailed model of what is "normal". It can then quickly detect cases where there is some significant deviation from the norm. The tool does not "understand" what is abnormal, or even whether it really represents a threat of any kind. It is up to a human operator to make a judgment about that.

- The impact from a *security* point of view is that staff can be made aware of potential threats in a way that would have been totally impossible without the tool: humans could not possibly process the huge volumes of data involved. Thus: the tool gives a completely new way to detect threats.
- The impact from a *safety* point of view is that early warnings to security staff give them the opportunity to react quickly and thus decrease the probability that the threat will actually arise and cause harm.

The IMPETUS **Bacteria detector** continuously monitors air samples to detect cases of abnormally/dangerously high levels of bacteria, such as would arise in the case of a bacterial attack. Automated detection of this kind was not possible before: attacks would first be noticed when citizens started to show symptoms of infection.

- The impact from a *security* point of view is that staff can be made aware of the danger automatically and immediately, and initiate response measure without delay. This was not possible before.
- The impact from a *safety* point of view is that the threat can be contained to the location at which it occurred, with affected victims being quarantined and/or disinfected. Without the early warning provided by the tool, infected persons would move out into the community and the infection could spread very quickly to large numbers of people.

2.2.2 Increased probability of detection of threats

The IMPETUS **Firearm detector** continuously monitors surveillance camera feeds and automatically creates an alert if a firearm is detected in a public space. The alert shows the exact location and appearance of the potential attacker, and this can be timely shared with colleagues.

- The impact from a *security* point of view is that the probability of staff noticing a potential threat is much higher (it is not feasible to stare for long periods at screens showing CCTV feeds), and that the response can be faster and more effective.
- The impact from a *safety* point of view is that the improved effectiveness of security staff decreases the probability of becoming a victim of a gun attack.

The IMPETUS **Social Media Detection** tool scans large volumes of text on social media and other public online sites, looking for topics/keywords that might indicate potential trouble or threats. The results of this analysis are presented to intelligence staff, who can assess the situation, perhaps carry out further investigations, and set up any necessary response or presentative measures.

- The impact from a *security* point of view is that the probability of staff noticing a potential threat is much higher (it is not feasible to monitor huge volumes of data on social media), and that steps can be taken to prevent or mitigate potential threats.
- The impact from a *safety* point of view is a reduction in the probability of dangerous situations arising.

2.2.3 Improved ability to manage specific security operations

The **IMPETUS platform** integrates multiple tools in a unified interface so that security staff who need to interact with multiple tools can do so in one place. Furthermore, this unified interface can be shared amongst multiple staff, which supports *common situational awareness* – well-known to be one of the key factors contributing to effective security operations. Indeed, the IMPETUS platform can provide information in a timely and accurate manner to ensure effective decision-making and promote transparency and accountability. Therefore, it is imperative that information is conveyed promptly and with a high degree of accuracy to all the relevant stakeholders and decision-makers. The increased level of automation and information sharing will impact the working processes for security staff, making them able to *work more efficiently* and *communicate more effectively*.

The IMPETUS **Evacuation optimiser** provides instant advice to security staff on how to effectively manage an evacuation (e.g., advising on which routes to favour/block). It does so based on simulations of different

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.

evacuation scenarios carried out as part of preparedness work. This allows security staff to work more effectively in managing evacuations.

The tools illustrated in this section have their primary impact in terms of security (making staff more efficient), but there is of course an indirect impact on safety from anything that improves effectiveness of security staff.

2.2.4 Improvements in operational efficiency of security staff

The IT infrastructure of a city is of crucial importance to all sorts of operations in the city – including security operations. Two IMPETUS tools –**Cyber Threat Intelligence** and **Cyber threat Detection and Response** are designed to identify possible threats and vulnerabilities in IT systems. Use of these tools has an impact on reliability of IT systems and thus on the ability of security staff to do their work effectively.

Security operations are, however, dependent not only on technological solutions but also on *people*. People do not work effectively if they are over-worked and stressed – or indeed under-worked, bored and inattentive. The IMPETUS **Workload Monitoring System** measures mental workload and stress of emergency operators using a brain-computer interface, and raises alerts if anomalies arise. The brain-computer interface is based on a simple headband that can be worn comfortably by security staff while working. This tool minimizes potential human error and improves human-machine teaming performance by monitoring the physical, emotional and mental workload status of operators while they perform their duties. It provides an early notification of an individual and/or team's workload capability and ability to cope with stressors during emergencies.

The effectiveness of security staff also depends on education/training and on organisational issues related to working processes. IMPETUS can have a positive effect on these issues through use of a non-technical result of the project: the IMPETUS **Practitioners Guides**[1]. The Practitioners Guides are an online resource offering practical advice on issues related to security, including ethics, overall operations and education on cybersecurity; they will be extended and updated based on experiences and new developments. Making information on these topics easily accessible and up to date will have a positive impact on overall effectiveness of security staff.

More generally, adoption of IMPETUS tools will also have an impact on the working environment and everyday work-life of operators because they remove several of the stress factors that operators must deal with. Removal of manual and repetitive processes also gives staff the opportunity to devote more time to strategic tasks that are more rewarding for them personally and more directly useful for the organisation.

The results illustrated in this section have their primary impact in terms of security (making staff more efficient), but there is of course an indirect impact on safety from anything that improves effectiveness of security staff.

2.3 Improvements in *perception of* safety and security

The section above has shown that we can expect real improvements in security and safety through adoption of IMPETUS (or technology of the same type from other sources). But will members of the public *feel* safer as a result? That is a more difficult question to answer.

We could consider it simply and assume that improvements as described above will gradually become apparent to people, making them increase their trust in the effectiveness of security services and thus feel safer. But there are factors that can work against this:

- Improvements in safety will often mean that something that might have happened does not happen. It is the absence of something, rather than the presence of something, that is the "evidence" of improved safety. But "absence" is not very newsworthy, and it might only receive media attention in things such as annual crime statistics, or occasional changes in "threat level" published by governments. On the other hand: if some kind of major incident such as a terrorist attack occurs and results in deaths, injuries and damage– that will receive massive publicity. There *might* be an opportunity for the authorities to explain that some even worse outcomes had been prevented through good working practices and use of smart technology. But it is unlikely that people will feel safer because of that: they will tend to focus on the negative outcomes that actually happened.
- Changes and events occurring in the wider society may lead to increases in crime levels and terrorism. And if those increase, citizens may experience increases in threats and negative outcomes – even though

[1] https://impetus-pg.atlassian.net/wiki/spaces/IPG1/overview

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.

improved security might in reality be helping to limit it. The argument that "it could have been even worse" will not make people feel safer.

Our conclusion is that a positive impact on perception of safety will depend on the authorities being pro-active in "selling" the benefits to citizens – both in terms of explaining what is being done and providing evidence of progress that has been made. When considering aspects of ethics and privacy (see chapter 3) it will anyway be necessary to establish a dialogue with citizens; this could provide an opportunity to promote the benefits.

2.4 Possible negative impacts

If IMPETUS tools (or similar tools from other sources) work in the way they are designed to, we do not see any potential negative impacts on safety and security.

But what if a tool fails to work properly (e.g., totally fails to detect the danger it is designed to detect, or provides responders with inaccurate information about the location, …)? And what if its failure leads to a negative outcome? That incident in itself would not necessarily be a negative impact on security and safety (it might have happened anyway without the tool, so we are not worse off than before). But if information about the failure becomes public knowledge, there could potentially be a negative impact on perceptions of security and safety – criticisms would emerge such as "look – the authorities are spending lots of money on fancy tech to protect us – and see what happens!".

To avoid negative impacts of this type:

- Technology must be developed in a collaborative manner with users and relevant authorities to ensure that local, national, and European regulations are adhered to. This will help to ensure compliance with regulatory requirements and promote responsible and ethical technological innovation.
- Technology must be thoroughly tested and configured properly for local conditions.
- Users must receive detailed and continuous training in its use.
- Users must be made aware of boundary limitations in the technology.
- Working practices must be adapted to make optimal use of the technology in operational practices.

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 Adherence to sound ethical principles and respect for privacy

Work on ethics was a core part of the work in the IMPETUS project.

There were major efforts to ensure adherence to ethical principles and privacy regulations (e.g., GDPR) in *carrying out the work of the project during its lifetime.*

Ethics work in the project went beyond project activities to also consider **the ethical and privacy challenges involved in wide-scale adoption of technological solutions for public safety, including AI-based technology**. That is the scope of this chapter.

3.1 Improvements in ways of dealing with ethical and privacy issues

Concerns about ethical issues and data privacy can act as a major obstacle to adoption of new technologies, especially in sensitive areas such as security and in cases where surveillance of citizens is involved. These factors apply in the case of some of the IMPETUS tools. To overcome them, it is necessary that authorities responsible for security, and other decision-makers in cities, have greater awareness and understanding of the issues, and ways of dealing with them. The project can have impact on this as follows:

1. *Demonstrating feasibility.* The two trial events and the two large scale exercises in the pilot cities in the project, and the preparatory work for them, showed that it is possible to apply the types of tools developed in the project in an ethical way, and adhere to relevant legislation on data privacy.
2. *Education and increasing awareness.* Based on lessons learned in the project, and other sources, the project has created a section on ethics in the online **Practitioners Guides** (see section 2.2.4). This is aimed at both potential and actual adopters of IMPETUS results (and other similar technology). It will make it easier for users to understand the issues, ways of dealing with them, and resources available to help in the process.

3.2 Possible negative impacts

Even if IMPETUS (or other similar) tools are implemented with all due care to ethical and privacy issues, citizens may nevertheless react negatively, perhaps very negatively. Many people simply *do not like surveillance*, neither in public spaces nor online (both of which apply in using IMPETUS tools). The individual freedom of citizens needs to be respected.

People can be sceptical to the argument that "we are doing this for your own good, your safety" and be suspicious that promises (e.g., about images being anonymised and deleted after a given period) may simply be lies – that the authorities have some other agenda.

The prevalence of attitudes like this can vary from one country/city to another – but they are never completely absent.

It can also happen that information is easily misunderstood. For example: some AI-based image processing systems use facial detection. The role of that is to understand which part of an image is a person's face – in order to blur that part of the image. The intention is actually good from a privacy point of view – to prevent identification. But already suspicious listeners don't catch the nuance between facial detection and facial recognition. The latter is about deliberately using the image to determine the identity of someone in a public space, and raises serious privacy and other ethical concerns.

Any use at all of images that include people can also raise concerns in the population about possible racial or other bias.

We could also speculate about whether, if people become aware of some kinds of monitoring, it might affect their behaviour. For example, if people object to monitoring of social media posts (see **Social Media Detection** tool, section 2.2.2) it could lead to them switching to other ways of communicating using channels that are more difficult for security staff to monitor.

3.3 Necessity of dialogue with citizens

In view of all of the above, it is important that authorities engage with members of the public, both at the local and the national level. The core issue is that some balance has to be struck between the advantages of improved

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.

safety and the perceived intrusion of increased surveillance. There is no perfect solution, and there will always be people who think there is too much or too little of one or the other. Dialogue with citizens must be:

- Open and transparent.
- Two-way, and open to compromise.
- Clearly communicate how the technology works – including its advantages for security, its limitations, and built-in safeguards.
- Demonstrate not only conformance with formal regulations/laws, but also that interventions are necessary and balanced compared to perceived threats (which may vary from place to place).

It is recommended and highly desirable to involve citizens, or at a minimum, organizations representing them, in projects of this nature. The participatory approach would foster a sense of ownership and engagement among citizens, providing them with the opportunity to actively participate in the development process, and share their expectations, concerns, and vision. Such a collaborative approach would ensure that projects are more reflective of the needs and aspirations of the wider community, and that they are designed and implemented in a more inclusive and participatory manner.

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 Gender equality

Gender equality is a fundamental value for both the UN [1] and the EU [2, 3]. When it comes to safety, there is lots of evidence that women and men experience threats and feelings of insecurity differently. In addition, women are exposed to harassment and sexual violence to a greater extent than men. Harassment and violence against women have been a societal problem for a very long time, and the media focus is often directed at describing how women feel unsafe in public spaces. This feeling of not being safe ultimately contributes to many women avoiding public spaces, and therefore limits their freedom of movement.

There are several factors that can contribute to making public spaces safer. Better lighting, shorter distances to transport, visible law enforcement and video surveillance are just some of the factors often mentioned as possible measures that will increase city security for women.

At the most general level, adoption of technology such as IMPETUS aims to increase security in public spaces. While not specifically targeting women, the technology will have a positive impact on general levels of security and safety (see chapter 2) - and that may contribute to women feeling more safe and secure. And that can have impacts in terms of:

- Reducing the existing gap between men and women about perception of safety.
- Reducing limitations on freedom of movement for women.

In terms of employment, the security sector has traditionally been somewhat male dominated. The introduction of technology such as IMPETUS will lead to changes in working practices and roles in some security operations. It is *possible* that this might contribute to work in the security sector becoming more attractive for women – but we have no specific indicators at the moment to suppose this might be likely.

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 Financial

5.1 Costs of security staff

As described in sections 2.2.3 and 2.2.4, adoption of technology such as that offered by IMPETUS can have an impact in terms of increased effectiveness of security operations, with a greater degree of automation of some work processes. Some might consider that this might lead to opportunities for financial savings – less staff would be needed. We consider that this is unlikely since *these technologies are aimed at empowering users* and not replacing them. Therefore, it is also unlikely predict that authorities would see the benefit as being improvements in security for the same staff costs. Thus: our prediction is that there will limited if any impact on staff costs.

5.2 Financial costs to the community

The costs of crime or other threats to public safety are usually most obvious in terms of human tragedy for victims and their families. While it is never possible – and could even be regarded as distasteful – to accurately measure human tragedy in financial terms, the reality is that there are financial consequences of crime and terror attacks.

In IMPETUS deliverable D9.3 *Business cases* we report on a detailed analysis of the estimated financial costs of crime in the two pilot cities in the project, Oslo and Padova. The deliverable also makes estimates of the possible contribution to limiting these costs that could arise from improved security arising from IMPETUS. While these are *very* rough estimates, we consider that it is clear that there can be a significant and positive financial impact of adopting technology such as IMPETUS.

5.3 Possible negative impacts

Adoption of technology such as IMPETUS also brings with it new costs: the technology itself is not free, and time is needed to train staff and adapt working processes. This needs to be taken into account in calculation the overall financial balance. This is estimated very roughly in deliverable D9.3, which concludes that the balance is most likely to be positive (especially over time).

As mentioned at the start of this chapter, one could also speculate that there might be a negative impact on employment (fewer security staff). We consider this to be unlikely.

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 Public policy

There is an expectation that research projects that receive EU funding should substantiate stated policy goals and contribute to solving our common societal challenges.

IMPETUS results contribute to social impact on issues highlighted in public policy both at European level and globally. In particular, the UN's goals for sustainable development and the EU's investment in digitalisation are relevant:

- UN sustainable development goal #11 *Sustainable cities and communities - Make cities and human settlements inclusive, safe, resilient, and sustainable* [4].
- UN development goal #5 *Gender equality* [4].
- The EU Security Union Strategy. The EU prioritises to strengthen its overall security architecture, which aims to enhance protection of EU citizens. The Fifth Security Union Progress Report [5] shows that significant steps have been made in strengthening the protection of critical infrastructure from physical, cyber and hybrid attacks, in fighting terrorism and radicalisation as well as in the fight against organised crime. IMPETUS will contribute to further progress in this area.
- The EUs Urban Agenda for public Security partnership [6].

Adoption of IMPETUS results can also contribute to the Critical Entities Resilience Directive (CER)[2] that formally came into force on 16th January 2023. This directive relates to protection of critical physical infrastructure and includes requirements on quality control of security services. Using IMPETUS (or similar) technology can improve the effectiveness of security staff, and thus facilitate passing quality control tests.

IMPETUS is also relevant to the NIS 2 directive[3] (December 2022) that aims to achieve a high common level of cybersecurity across Europe. The two IMPETUS cyber tools (**Cyber Threat Intelligence** and Cyber threat Detection and Response – see 2.2.4), and the cybersecurity part of the **Practitioners Guides** (see 2.2.4) are relevant here.

[2] The Critical Entities Resilience Directive (CER) website
[3] The NIS 2 Directive website

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 Employment

We do not foresee that there will be any significant impacts on employment. See also section 5.1.

8 Climate and environment

We do not foresee that there will be any significant impacts on climate or environmental issues.

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 Conclusions

The adoption of the technology developed in IMPETUS, guided by the principles described in the project's *Practitioners Guides*, is likely to lead to significant positive societal impacts in the areas described in this report. The extent of the impact will be considerably amplified by adoption of similar technology from other sources (currently existing and emerging in the future). IMPETUS has a role in encouraging adoption of results from other sources, by having shown in the project that such solutions really can work in practice.

Achievement of the positive impacts is to some extent dependent on the way in which adoption of technology is presented to the public – both by the authorities themselves and the media.

There are also, as outlined in this report, some potential negative impacts. However, we consider that the positive impacts are likely to outweigh the negative ones by a considerable margin.

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.

References

1. United Nations Development Programme (UNDP), *"Human Development Report 2020: The Next Frontier: Human Development and the Anthropocene"* – December, 2020 (https://hdr.undp.org/content/human-development-report-2020).
2. European Institute for Gender Equality (EIGE), "*The EU's evolving legal and policy approaches to Gender Equality*" – October, 2022 (https://eige.europa.eu/publications/eus-evolving-legal-and-policy-approaches-gender-equality).
3. European Commission, "*The European Pillar of Social Rights in 20 principles*", Chapter I: Equal opportunities and access to the labour market – Section 2: Gender equality, November, 2017 (https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/economy-works-people/jobs-growth-and-investment/european-pillar-social-rights/european-pillar-social-rights-20-principles_en).
4. United Nations, Department of Economic and Social Affairs Disability, *"#Envision2030: 17 goals to transform the world for persons with disabilities"* – September, 2015 (https://www.un.org/development/desa/disabilities/envision2030.html).
5. European Commission, "*Fifth Progress Report on the EU Security Union Strategy*" – December, 2022 (https://commission.europa.eu/publications/fifth-progress-report-eu-security-union-strategy_en).
6. *The Urban agenda for the EU – Security in Public Spaces* (Orientation paper) – January, 2019 (https://ec.europa.eu/futurium/en/system/files/ged/orientation_paper_security_in_public_spaces_public.pdf).

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
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.