IMPETUS Newsletter

Issue 4, March 2023

Welcome to IMPETUS – improving security in public spaces

IMPETUS is a Horizon 2020 Research and Innovation project aiming to help city authorities improve security in public spaces. Our newsletters aim to keep you up-to-date about project goals and achievements, and perhaps encourage you to get involved in our work or (later) use our results.

If you are in involved in public safety – directly or indirectly, as a potential user or as a potential supplier – IMPETUS surely has something for you!

Find more on our website
https://www.impetus-project.eu

In our fourth newsletter:

- **Thomas Robertson** also tells us what IMPETUS can do for the future of **Smart City Technologies** for Resilient Cities.
- An account of our **"Final Dissemination Event"** held 30–31 January 2023 in Rotterdam, The Netherlands. We also chat to **Oskar J. Gstrein** and **Bente Skattør**, in COSSEC, about their views on the **IMPETUS Solution**.
- **Manuela Soccol, Jelena Radošević** and **Alex Townsend-Drake** also reflect on the IMPETUS Project.
- Did **COSSEC** function well for IMPETUS? We hear from **Sandro Bologna**.
- **Joe Gorman** reflects on the **IMPETUS Journey**.
- Also in this Newsletter: News in Brief and Forthcoming Events.

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

IMPETUS and the Future of Smart City Technologies for Resilient Cities

What IMPETUS Tells us About the Potential for Smart City Technologies and the Way Forward for Realizing this Potential?

THOMAS ROBERTSON

CEO of Thinking Teams
Director (North America Region)
TIEMS

IMPETUS brought together a large group of experts and stakeholders to work on the challenges of applying advanced technologies to improve safety during large-scale urban events.

Operational people learned about the potential of these technologies to help them in their work. Technologists tested their products and ideas against operations and learned what it will take to move from demonstration to operations. New and valuable personal networks were established.

IMPETUS has produced a wealth of information detailing these lessons and others, and a large network of people ready to carry the ball forward. We look forward to this legacy contributing to safer cities through advanced technologies.

What have we learned on the 30-month journey that was IMPETUS? Undoubtedly each of us individually has learned many things. However, through our collective efforts we produced results that contribute important insights illuminating the path ahead. Here are some examples:

- We verified that there is a huge potential benefit from the use of smart city technologies for urban safety. Our analysis confirmed that investments in these technologies will likely be returned many times over.
- During our demonstrations and exercises, smart city operators showed they could learn and use IMPETUS technologies, and they became convinced these technologies could add value to their operations.
- Technology developers became better aware of the challenges they face in fielding operationally effective systems:
  - Variability in operational environments makes it hard to develop robust systems using machine learning. Extensive on-site training will probably be required.
  - Assessing operational effectiveness and estimating return on investment is difficult because testing with real data in real situations can be expensive and operationally prohibitive.
  - Taking advantage of advanced technology may require a sizable investment to integrate it with existing technical systems and data sources.
- While technology provides new opportunities for collaboration and information sharing across individuals and groups, these collaborators may need to first agree on shared terminology.

Reflections on Smart City Technologies

ALEX TOWNSEND-DRAKE

CTPN Head of Programme
Counter Terrorism Preparedness Network

Alex is a member of COSSEC, and he has joined all COSSEC meetings throughout the project period, and continuously given feed-back to the project from the "outside world".

In the wake of the cold war, Henry Kissinger said: *"Never before has a new world order had to be assembled from so many different perceptions…and the exploding technology of the contemporary period".*

Today, we continue to face global crises with strategic implications for security – COVID; Taliban-rule in Afghanistan; the war in Ukraine; climate change; and economic instability to name just a few. Most notably for today, we are also being pushed towards a significantly more automated world, where new technologies are fusing the physical, digital and biological. This convergence poses new threats and opportunities for society and cities; layers of structures, systems and services that are dependent on this infrastructure.

On the one hand, rapid technological advancement offers tools that can be harnessed, on the other they create risks and dilemmas. Deloittes report on 'Making Smart Cities Cyber Secure' noted that the convergence of physical and online worlds enable cities to coordinate through remote cyber operations but this exponentially expands the cyber threat landscape. This is coupled with a European Commission report on 'The Landscape of Hybrid Threats' that highlighted how "cyberspace [and therefore many technologies] provides a new delivery mechanism that can increase the speed, diffusion and power of an attack".

Indeed, it is only when technologies are attacked, or they go wrong, that we are reminded how powerful they are. Yet they have unprecedented potential and value – operationally and strategically.

If technological solutions for security are to be accepted and adopted by cities, authorities, and citizens, we need to know (1) how technology can help shape security and operations, (2) be harnessed to support urban design, and (3) remain beneficial and maintain an ethical standing. The challenge is demonstrating and evidencing that those involved are Proportionate, Legal, Accountable, Necessary and Ethical.

REPORT:
The IMPETUS Final Dissemination Event

The future of urban security: Urban planning and adoption of advanced technological solutions

30–31 January 2023
Rotterdam Hilton Hotel, Rotterdam

We are delighted to announce that the project's Final Dissemination Event in Rotterdam, The Netherlands, 30-31st January was a great success!

This event was organized with the support of the Secu4All project. Secu4All is coordinated by Efus (European Forum for Urban Security) and funded by the European Union's Internal Security Fund — Police. Some 70 participants from IMPETUS, COSSEC and Secu4All gathered to discuss the future of urban security and the potential role of advanced technological solutions in urban planning and city daily life.

Members of the research teams, representatives of interest organizations and representatives of the management of cities and municipal organizations discussed the progress and results of IMPETUS and other relevant research projects about safe and secure cities.

Mingling and discussions over drinks and snacks on the first evening of the Event at the Hilton

The core theme of the event was improving safety in public spaces in urban environments. The event had three main goals:

1. **Networking**: To bring together actors in the field (the organizing projects, other projects, municipalities, law enforcement, policy makers, …) to share results and experiences, and to establish co-operations for the future.
2. **Increasing awareness:** Help stakeholders understand the potential and challenges of adopting technological and non-technological approaches to urban security by presenting and discussing what we have achieved and learned in IMPETUS, Secu4All and other projects.
3. **Moving forward:** Explore ideas on how potential barriers to adoption of new approaches (including ethical concerns) can be overcome; identify what future steps are needed before the full potential can be realized.

The two days covering these goals were busy ones...For Secu4All members and some other invited guests, the event started with a "field visit" to Rotterdam. After some introductory presentations, the field visit continued with a "walk-and-talk" around the Rotterdam City Centre, looking at the mitigation strategies preventing insecurity in public spaces. This afternoon session was followed by an evening project poster session that gave guests the opportunity to mingle and network with some refreshments and light snacks.

The Program of Day two was:

Introduction & Welcome

- About IMPETUS

- About Efus/Secu4All

Adopting technology for urban security – how did it go and what did we learn?

Provide insights into practical experiences and lessons learned from introducing technology in pilot cites in the context of EU projects.

Dilemmas arising at the intersection of Security, Technology and Society –and how to approach them

Is adoption of hi-tech solutions for security acceptable to European citizens? Law enforcers and other security personnel? City authorities? Policy makers?

Exhibition: Key results of the IMPETUS project

Showcase IMPETUS results, highlighting for each: • Capabilities & innovation; • Potential role in the wider context of urban security; • Current level of maturity & development plans

Facilitating widespread and responsible uptake of new approaches to urban security

Examine the factors that could stand in the way of successful adoption of new approaches to urban security for resilient cities and consider what can be done to make things easier.

Quo Vadis – where do we go from here?

• Consolidate lessons learned from the day

• Dream about the future

The second day started with ***"Introductions and Welcomes"*** with presentations by both Joe Gorman (SINTEF, IMPETUS Project Coordinator) and Pilar De La Torre (Efus, Secu4All Project Coordinator).

The session on ***"Adopting technology for urban security – how did it go and what did we learn?"*** included presentations/videos about the work carried out, as well as open discussions about experiences and views on the benefits and challenges faced in introducing technology in pilot cites in the context of EU projects.

Project participants together with people from cities and other potential users

Joe Gorman (SINTEF, IMPETUS Project Coordinator) introducing the IMPETUS Tools

Project partners showcasing their IMPETUS Tools at the Exhibition in an interactive and integrative fashion

In the last panel session **"Facilitating widespread and responsible uptake of new approaches to urban security"**, we examined the factors that could stand in the way of successful adoption of new approaches to urban security for resilient cities and consider what can be done to make things easier.

In the final open discussion session, **"Quo Vadis – where do we go from here?"**, we dared to dream about what the future may hold for the technologies, IMPETUS, Secu4All, COSSEC....

Jaroslav Pejcoch chaired the last panel session

This event showed what was achieved in the organizing projects (both in terms of technology and other aspects) and placed these achievements in a wider context. Concerning technology, we are proud of what we have developed and demonstrated in IMPETUS. But other tools exist, and new ones will surely emerge in the future. At this event, we looked at the broader picture – even dreamt a little – about what the future may bring.

We asked some of the attendees to write a few words about their reflections and experiences from the event...

Ethical Dilemmas and the Use of Security Technology

MANUELA SOCCOL

Ethics Manager
IMPETUS Project
&
Technology Transfer Attorney
University of Padova

Manuela Soccol is an Italian lawyer expert in the legal tech. She helps private and public entities to deal with data protection and ethics issues related to the implementation of new technologies. Manuela was on the panel at the Final Dissemination Event dedicated to **"The future of urban security: urban planning and adoption of advanced technological solutions".**

A specific and extensive panel discussion during the event allowed project partners and external guests to share different perspectives on ethical challenges that the use of new advanced technologies and of artificial intelligence may present. All our panellists had different backgrounds: there were people working for public forces who work for urban security, technology developers and lawyers, both internal and external to the project. The panellists tried to answer questions such as how to find the balance between security and autonomy, which role do cultural and political differences play, how can ethical principles and legal frameworks inform a trustworthy use of security technology.

On one hand, it appeared clear that we must face an unavoidable and maybe unsolvable dilemma between security and the protection of the freedom of citizens. On the other hand, technologies are continuously developing, and they concretely help in the prevention of crimes, but governments should focus on the measures to be taken to prevent citizens from considering them as new threats, instead of useful tools. Here comes another challenge: how can governments know how citizens feel in this regard? How can we work on developing European legislation and ethical standards, when stakeholders have so many different points of view?

In any case, in the future years, it will be of greater importance to involve citizens in decision processes, also to inform them and to prevent the "fear of the unknown". For instance, surveys that were organised at national levels in some countries and also within the IMPETUS project itself show that many citizens would be opposed to the monitoring of social networks by public authorities but are less concerned when the entity controlling them is a company with marketing purposes. Indeed, the way social networks work and

perform shows that many citizens are willing and not scared to share their personal data with undetermined subjects.

Will we ever have final answers to these issues? Probably not: technology evolves always faster than laws and regulations. A possible solution may be to focus on adapting shared general principles of European society to the use of new technologies and of artificial intelligence to define the criteria to find the balance among them and the path to be followed in further developments. We need to respect the basic principles of necessity, lawfulness, and responsibility but there is still the need to examine how to concretely apply them in new contexts and in a multicultural society. A fundamental document is represented by the "Guidelines on trustworthy AI", which is also well-known by tech developers. But even these Guidelines are hard to be applied: for instance, to pursue transparency and explainability in the functioning of algorithms, AI may lead to less accurate and less trustworthy results and decisions.

Some opinions were shared also on the topic of algorithms' bias. AI-developing companies should make a big effort to grant diversity, non-discrimination and fairness through the choice and definition of input data and algorithm design. It is still an open question whether it is possible to train an AI without biases using training data that are selected by humans which will unavoidably have biases.

The dilemma is still open… and unsolvable. One possibility is to consider the dilemma from another perspective. As citizens we should have not only the right to live in a safe city but also the freedom to live in a safe city. In other words, the right to live in safe cities should have the same importance as the freedom of movement or the rights to private and family life. If we don't have the possibility to live in safe cities, we couldn't be free to move. Nowadays, the urban safety needs new technologies, and the new technologies need AI.

Facilitating widespread and responsible uptake of new approaches to urban security

JELENA RADOŠEVIĆ

Representative
Institute for Security Policies (project partner)

Jelena Radošević attended the panel discussion on **"Facilitating widespread and responsible uptake of new approaches to urban security"**, and reports on her experience of the event.

Contemporary technological advancements create new opportunities for enhancement of urban security. However, uptake of new approaches and tools by the public sector is not that easy or common. Why isn't it? What are the challenges and how to address them? These were the questions the panel on Facilitating widespread and responsible uptake of new approaches to urban security tried to answer by gathering opinions and experiences from Osman Mohammad Ibrahim (The City of Oslo), Lawrence Schaetzle (European Forum for Urban Security, Efus, network dedicated to fostering discussion, cooperation and support among local and regional authorities in the field of crime prevention and urban security), Sachin Gaur (BMA, standardization expert) and Joaquin Garcia-Alfaro (IMT, coordinator of the Practitioners Guides, a solution provided by the IMPETUS project), moderated by Jaroslav Pejcoch (The International Emergency Management Society).

The biggest challenge seems to be that the Cities in general are not well informed, not completely aware of technology advancements potentially useful for the enhancement of security in their cities nor do they regard use of contemporary technology in the security sector as essential.

Introducing something new inevitably means changes in the system: effort, money and time investments; so there must be a really good reason to embark into such endeavours. One must also be careful, as the use of new technology could bring some new (cyber, data privacy breach) threats

to the City (systems). In addition, technology is developing much faster than the City systems adaptation capacity in daily operations is, which makes its use rather complex.

From the experience of the City of Oslo, it is the sense of emergency that makes things happen. We've all witnessed an increase in the development and use of technology by public services and trust in it by the citizens during the COVID19 pandemic. In normal times, the sense of urgency can be created through an exercise. Efus offers the Cities a sort of urban security package that includes provision of vulnerability assessment, which is of great interest to majority of the Cities, and with it, information and education on urban security by design, contemporary technological tools for urban security enhancements etc. The transfer of knowledge and co-creation of City-specific solutions is done in a very creative, interactive, participatory manner, including storytelling and serious gaming methods, with great respect for local specifics and the people involved. When talking about informing people on the use of technology in the security sector, it is important to emphasize the advantages such as automatization of procedures, time efficiency and precision, but also to accentuate the risks, where to be careful and how to prepare for the risks in the best way possible. In India, a hackathon on urban security was organized that invited and included the citizens in finding the best solutions, and therefore making the results as site specific as possible and breaking the potential of negative public attitude of the citizens on the use of technology in the field of urban security.

The key to this is standardization, which allows the systems in cities to grow smoothly with new technologies and modules, and also allows local companies or universities to be creatively involved in the development of the system. It is definitely not easy to introduce new technology for it to be used by the Cities in the security sector, and it is far easier to talk about it with the Cities that have already invested some time, money and efforts in that direction, usually as a result of their own local needs, but EU funds incentivizing projects on use of technology in urban security sector, provision of accurate information on benefits of use, but also quality preparation for the reduction of risk and misuse of it, and quality approach through interactive trainings and emergency simulation exercises are slowly guiding the Cities to uptake technology in an responsible, ethical, logical and user-friendly way.

We asked some of the attendees to answer a few key questions about their experiences in IMPETUS. They kindly agreed to help...

What are your thoughts?

OSKAR J. GSTREIN

Program Director & Assistant Professor
University of Groningen

https://www.linkedin.com/in/oskar-j-gstrein-026a34248/

Oskar J. Gstrein is a member of COSSEC, and Chaired the session on "**Dilemmas arising at the intersection of Security, Technology and Society – and how to approach them**".

Question 1: One of the most difficult trade-offs between security requirements and technology solutions is in the impact of Ethics' Could you tell us some ethical considerations that you think are most important to satisfy?

I think there are two issues which are really important. First, we need to make sure that technology remains human-centred. In the past I did research with industrial designers, and they used the example of a plane which has to be planned in a way that it supports the pilot to bring the passengers to their location. It is not the plane which takes the passengers there, it is the pilot and the crew. Similarly, we need to make sure that emerging technologies are contributing to a clearly defined problem and solution, instead of becoming the issue themselves.

Secondly, one of the big ethical challenges we face is how to include the legitimate group of stakeholders in discussions around problem analysis, identifying requirements, regulating and shaping societal implementation of the technology. A good example here are COVID-19 tracing apps, which have been rolled out at light speed in many countries, but with little consideration of how they actually shape the behaviour of the people and institutions who are supposed to use them and follow-up on the notifications.

Question 2: Data-driven approaches to human decision-making introduces bias in inputs, outputs and processing: Can you express some considerations about the ethical principle of Perceived Fairness?

Here I have to think of the famous saying by Lord Hewart: "Justice must not only be done, but must also be seen to be done". Certainly, in democracies which function under the rule of law and look as fundamental rights as one of the pillars of their society, it is important that public decisions are explainable. For AI and Machine Learning, this is a big challenge since much of their appeal steams from the fact that they identify correlations in ways and numbers that is difficult for humans. So, we must find a way to make the systems more explainable, but also reconsider where

explainability is absolutely necessary and where such technologies are simply not fit for purpose…. The fundamental question on whether machine learning and automated decision-making systems should be used for all tasks remains open, and needs more consideration. Finally, the systems used should also be properly tested before they are deployed. We will see what the proposed EU AI Act adds to this once it is finalised.

Question 3: The right to privacy and protection of personal information should always be granted: How do you think that can be granted with the introduction of AI technologies?

The phrasing of the question is interesting, since privacy is a non-absolute right. In contrast to the prohibition of torture or slavery, privacy can be limited where this is based on a law, necessary in a democratic society, and proportionate.
When it comes to AI, the interesting aspects are often the predictions and inferences made about people. Maybe we need to think how the access to data can be limited by an individual so that certain data cannot be used for making such inferences. This could also be seen [as an] avenue towards data protection.

Question 4: According to your experience, how do you think the above principles have been satisfied with the IMPETUS technology and their use in the Security Operation Center?

As member of COSSEC I had the privilege to observe the Oslo simulation. While many innovative technologies where used, the 'dots' are still connected by people who also have the freedom to follow their experience and make independent judgments. Certainly, the increasing flow of information and the increased reliance on digital data make it also necessary to automate the filtering process increasingly, but it was still good to see that the platform remains human-centered in essence.

Question 5: Do you think it is appropriate to widely publicise the possible existence and capabilities of security systems and thereby reassure the public that their security is being taken care of, or at the same time raise concerns that personal rights may be violated, or do you prefer to build and operate such systems more in a classified mode?

To my knowledge there are two different camps on this question. Some say everything should be Open Source and available to the public to raise security levels, while others tend to protect their information and sources to avoid vulnerabilities. When it comes to the interaction with the public, it seems anyways more important to be clear about what systems do and what they do not do. This is a real challenge, since you would like to avoid that people change their behaviour because they feel constantly controlled and surveyed.

Question 6: Current AI security systems concentrate on data monitoring and pattern identification, at most, suggesting the next course of action. Do you think that we in time will get to the point where they also are active and automatically execute some actions?

At some point there will be practically autonomous systems, but it is difficult to say when and how exactly that will happen. The question of what it means to be autonomous is also difficult to answer. It seems to me that such autonomous systems will not be the most interesting systems for humans in the long run, and that the gradually increasing autonomy will open up the potential for hybrid statuses of human-machine interaction. These slightly different states of autonomy and automation will allow humans to interact with the systems in a way that might be much more enabling and stimulating, people might get the feeling that this is actually

useful for them. We already see this with cars, that get bit by bit more autonomous by having more assistance systems. Still, people have different preferences and use different levels of assistance. In contrast, the imagination of a chat bot where a user cannot distinguish whether it is a real person or not — the classical scenario of the "Turing test" — is just scary to most people.

What are your thoughts?

BENTE SKATTØR

Senior advisor (ICT & Business Development)
Oslo Police District

https://www.linkedin.com/in/bente-skatt%C3%B8r-61a8b039/

Bente Skattør is a member of COSSEC, and Chaired the session on **"Adopting technology for urban security – how did it go and what did we learn?"**.

Question 1: Many different technology providers are offering technology solutions claiming that they may help to increase security of Public Spaces: Do you have specific criteria to select such technology?

The Norwegian police must always adhere to the rules of public procurement. This applies to both traditional technology and AI solutions, ensuring compliance with the rule of law in Norway and relevant regulations, including GDPR for privacy and data protection… As the Norwegian police are in the process of considering AI solutions, the following aspects should be considered:

- ***Cybersecurity**: As public sector organizations are vulnerable to hacking, it is essential to ensure that potential vendors and partners have a solid reputation and are trustworthy providers of security solutions.*
- ***Ethics of AI in the Norwegian police**: There is a growing focus on AI ethics globally, particularly in the EU. IMPETUS has developed guidelines that are relevant for the Norwegian police. Currently, various units within the Norwegian police aim to participate in testing "The Toolkit for Responsible Artificial Intelligence Innovation in Law Enforcement," which will be launched by Interpol and UNICRI in 2023. As a*

I want to express my gratitude for the chance to be interviewed. At the same time, I want to emphasize that my responses reflect my personal understanding of the topics. My answers are based on my experience in innovation and applied research, with a focus on enhancing police work through the exploration and development of AI tools. Please note that my answers may not represent the official stance of the Oslo Police District or the Norwegian police.

member of that global working group, I am eager to learn about the results from the use of these tools...

- ***AI tools as a component of a technological platform**: Recently, there has been a significant advancement in AI tools that support safety and policing in smart cities... The challenge is to effectively integrate these tools and … deliver "the right information to the right person at the right time in the right context," much work remains to be done in partnership with citizens and other partners.*
- ***Multi-perspective and user-centred design**: In innovation, we aim for a multi-perspective approach with a strong focus on the end-user. End-user involvement is crucial as AI tools often result in significant changes to work processes. It is essential to keep the end-user in the loop, which requires continuous training and improvement.*
- ***Efficiency**: To ensure [efficiency], it's important to have effective tools and methods to measure the impact and estimate the return on investment of AI tools.*
- ***Synergies and scalability**: Key considerations for AI tools are their ability to find synergies with other tasks and their scalability to different locations and situations.*

Question 2: How do you deal with the controversial requirements of people asking for more security and more privacy at the same time: Do you have Guidelines about how to satisfy both requirements?

The Norwegian police must adhere to all existing Norwegian laws, regulations, and GDPR … The use of AI tools also poses challenges to existing laws and regulations. This has been seen in several countries, as demonstrated in the AI ACT EU and related debates. Therefore, it is crucial to increase our understanding of the legal implications of AI. Simultaneously, we need to push the boundaries and find innovative ways of developing AI tools while still complying with regulations.

Many people freely share personal information on social media platforms, yet they are wary of CCTV cameras in public spaces owned by entities such as municipalities, police, and defence. There is a need to better understand this phenomenon and potentially find mutually beneficial solutions through engagement with citizens.

The challenge of balancing security and privacy demands is complex. To help manage this challenge, consider the following strategies:

- ***Transparency**: Clearly and openly communicate with the public about security and privacy measures. Explain the trade-offs involved and decision-making processes.*
- ***Privacy by design**: Incorporate privacy considerations into the design, development, and deployment of security technology.*
- ***Use and evaluate AI Solutions**: Continuously monitor AI solutions to ensure they provide strong security and privacy protection… the criteria of which may evolve after implementation.*
- ***Educate and involve**: Engage the public on*

the significance of both security and privacy and empower them to protect their privacy and support security.

- ***Guidelines for the Security–Privacy Balance**: Establish a dynamic – or "living" – repository of guidelines and methods to balance security and privacy, which are digitised and rapidly updated in keeping with the rapid evolution of technology.*
- ***Risk assessment**: Regularly assess the potential risks to both security and privacy, and make informed decisions based on a comprehensive understanding of the consequences.*
- ***Independent/External audit**: Set up independent, competent resources to examine and oversee the application of security technology and privacy standards.*

Question 3: How do you deal with establishing a trade-off between introducing new technology and evaluating the impact on the Human Shift in the control room: Are humans really using the technology 24/7?

While humans use technology 24/7, balancing the introduction of new technology with evaluating its impact on human operators in control rooms can be difficult, but user-centred design, ethics and efficiency can help. It's critical for SOC operators to regularly rehearse and evaluate their performance to ensure they can effectively observe, analyse, and act quickly. Monitoring the stress levels of operators through performance monitoring both before and during the use of technology, using tools such as the IMPETUS Workload Monitoring System, is crucial in preventing adverse effects on human performance.

Question 4: According to your experience, what do you think could be the advantages and disadvantages of introducing IMPETUS technology in the Security Operation Centre (SOC)?

The adoption of AI technology in the Security Operations Centre (SOC) can bring several benefits such as:

- *Increased alertness, effectiveness and efficiency.*
- *Improved threat detection and response.*
- *Enhanced situational awareness.*
- *Improved decision-making.*
- *Scalability.*
- *Cost savings.*

While AI technology can offer numerous benefits to the SOC, there are also potential drawbacks that need to be considered:

- *Bias data, incorrect outputs and discriminatory consequences.*
- *Lack of human-based judgement and interpretation in different contexts, leading to errors or overlooked threats.*
- *Limited understanding and accountability for the actions of the algorithms and personnel.*
- *Job loss in the security sector due to AI automation leading to a reluctance in implementing AI tools.*

SOCs can address these to make sure AI tools are utilised in a way that improves security while protecting privacy and civil rights.

Question 5: Do you think the usage of advanced technologies simplifies or complicates the communication between the SOC and other organizations in a City?

The degree of difficulty in communication can greatly depend on the AI tools used. For example, if the AI tool is easily understood, such as computer vision or video analysis, where its identification of an object is visible, communication is simplified. However, if the AI tool involves complex algorithms, such as anomaly detection and pattern recognition, communication can become complicated if some stakeholders do not trust or understand the tool. On the other hand, I've found that physical co-location and collaboration among a diverse group of city representatives can enhance emergency management, especially during big incidents.

In general, the use of AI tools and advanced technology can simplify communication between the SOC and other organizations in a city in several ways:

- *The use of AI tools and advanced technology can simplify communication between the SOC and other city organizations in several ways:*
  - *Real-time data sharing enables faster and more effective collaboration, such as live video streaming at the scene using mobile technology.*
  - *Automated alerting reduces the time and effort needed to notify relevant organizations of potential security threats.*
  - *VR/AR collaboration allows for simulation of ongoing crisis/incident scenarios, regardless of physical location.*

Advanced technology in SOCs can also complicate communication in the following ways:

- *Resistance to change, where organizations are hesitant to adopt new technologies, slowing down adoption and complicating communication.*
- *Technical complexity and incompatible systems: AI tools can be complex and difficult to comprehend, causing difficulties for non-technical organizations to collaborate with the SOC. Different organizations may also use different or incompatible systems, hindering effective information sharing and collaboration.*
- *Not easy to use the AI tool (lack of user friendliness) in practice can result in mistakes that impact communication.*
- *Lack of training on the tool can decrease the ability to communicate and increase the risk of miscommunication or misunderstandings.*
- *The use of advanced technologies may introduce new cybersecurity risks, causing mistrust during communication.*

Question 6: What kind of information do you think is absolutely necessary for people in an emergency at various levels (citizens, police officer, crisis manager, chief of crisis staff, mayor)?

The question of providing the right information to the right people during an emergency… depends on the type of emergency and the roles and responsibilities of individuals involved and the situation. Delivering the right information, to the right person, at the right time and in the right context is a challenge; one that we'll struggle with for years to come. It is good to have a proper checklist what to do and exercise that – not to frighten people with inaccurate information.

IMPETUS outreach: Community of Safe and Secure Cities (COSSEC)

SANDRO BOLOGNA

COSSEC Chair
TIEMS

COSSEC has been a real success among IMPETUS activities. All goals set in the project for COSSEC have been reached. Up today COSSEC is made of 47 Members, mostly from Europe, but also from USA and India.

COSSEC Status (as of 21 February 2023)

Members: 47 Organisations
17 Cities
5 Citizen groups
14 EU countries
Activities: 3 Workshops
3 Webinars
2 participations in Live Exercises

COSSEC has organized three Webinars, addressing the three main aspects of urban security in smart cities, namely: Technologies, Processes and Ethics. COSSEC events have allowed exchange of experiences and best practices between stakeholders from smart cities. IMPETUS has contributed to the exchange of insights and viewpoints in support of the overall progress various on key issues related to public safety in smart cities. Among others, during the lifetime of the IMPETUS Project, COSSEC has established contacts with the European Forum for Urban Security (Efus), Urban Innovation Action (UIA), and URBACT – URBSecurity.

Particularly important was the participation of COSSEC Members to the IMPETUS Final Event, Rotterdam 30–31 January 2023. Twelve COSSEC Members participated in different roles. Two of them took part in the Field Visit on January 30th. Two of them played the role of Moderator in meeting sessions on January 31st. Four of them participated in the role of Panellists/Presenters in the different sessions of the meeting.

As IMPETUS draws to a close, we are looking at ways of prolonging the excellent cooperation and networking established in COSSEC. One possible avenue we are exploring is to establish a technical working group of some kind within Efus. Discussions on this possibility are at an early stage.

If you want to learn more about COSSEC, please contact:
Sandro Bologna, s.bologna@infrastrutturecritiche.it

Look Back, Look Around, and Look Forward!

JOE GORMAN

Project Coordinator
SINTEF

Joe gives us his reflections on the **"Impetus journey"**: what we have learned and the potential future of the IMPETUS solution.

As IMPETUS draws to a close, it is natural to look BACK at its beginnings. From the kick-off meeting in September 2020, the thing I remember most is how we wondered, as we all sat at home in uncertainty and various levels of pandemic lock-down: will we ever get round to trying out our ideas on the streets of our pilot cities? We genuinely worried that we might end up being a "paper" project that could only deliver documents from a gang of people who had never met.

That is why, for me personally, the high point of the project was in November 2021 when we had our first practical "acceptance pilot" in Oslo, and most of the partners met face-to-face for the first time. This was when we really started to understand the potential of the technologies being developed in the project, and realize that, yes, it was going to be possible to try these out in realistic settings. It was also when the consortium started to feel like a real team.

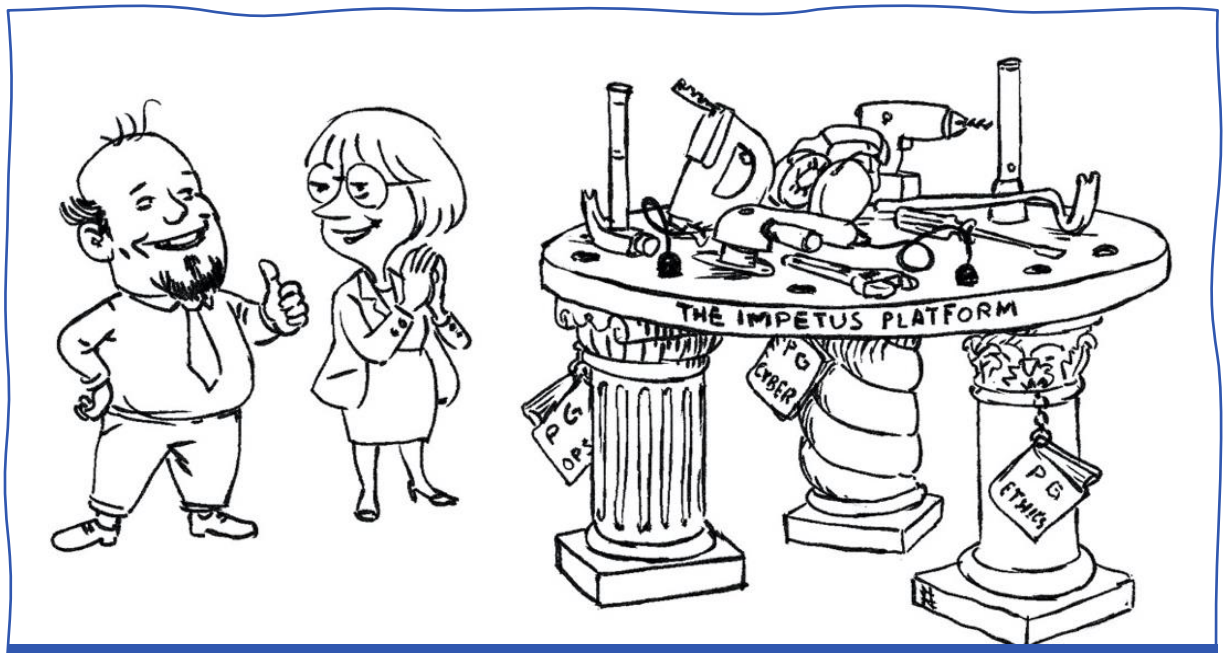
As time moved on, we were able to conduct further tests, in Padova and Oslo. We were also able to grow our COSSEC community and this way look AROUND – get feedback and views from multiple actors with different viewpoints from outside our own little IMPETUS club.

What, in the end, did we deliver? To start with, we delivered a set of tools, each contributing in its own way to improving safety in smart cities. Some are commercial products (or close to being so); some have a way to go before that. Common to all is that they demonstrate the feasibility of using hi-tech solutions for urban safety.

We also delivered an integrating platform that allows all our tools (and indeed other, existing tools) to interact with users via a common interface. A key lesson from our practical testing is that this integration aspect is vitally important to operational staff.

As well as technology, IMPETUS also delivers a set of three Practitioners Guides, offering practical advice about issues related to ethics, cyber security, and operations. The advice

they offer is relevant for any organization adopting technological solutions for urban security, it is not limited to IMPETUS. Still, we regard the "PGs" (as they are affectionately known in the consortium) as the three essential pillars on which the IMPETUS approach rests.



The three pillars supporting IMPETUS: Operations, Cybersecurity and Ethics
Artwork credit: Rafal Hrynkiewicz, Thales, Netherlands

One of our key lessons from dialogue with different users and different cities is that each city has its own needs and priorities: there is no "one size fits all" solution. Thus, IMPETUS does not try to provide a single, packaged solution. It rather provides you with some solutions that you might adopt now and some that you might adopt later, or combine with other solutions, old or new. Fundamentally, IMPETUS helps you to look ***FORWARD*** beyond what is possible now to what can be achieved in future through smart adoption of technological solutions.

News in brief

IMPETUS Practitioners Guides Release 1.1

2nd March 2023

The Practitioners Guides (PGs) provide guidelines, documentation, and training materials in the areas of operations, ethical/legal issues and cyber security. The Practitioners Guides are structured such that each area has its own Practitioners Guide (PG), namely the Practitioners Guide on Ethics & Privacy, the Practitioners Guide on Cybersecurity and the Practitioners Guide on Operations. They are presented in an online, browsable format that can be easily refined and extended over time. The IMPETUS Practitioners Guides can be accessed at: **https://impetus-pg.atlassian.net/wiki/spaces/IPG/overview**

IMPETUS–Barcelona "one-to-one"

24th February 2023

In the final week of the project, the Project Coordinator (Joe Gorman, SINTEF) and the Oslo city representative (Osman Ibrahim, City of Oslo) were hosted by Maria Vila Muntal of the City of Barcelona for a "one-to-one" meeting with public safety, police and fire service officials in the city. The goal was to present the IMPETUS solution and have a detailed dialogue on the potential applicability of IMPETUS (or similar) technology in a major European city. Discussions provided strong confirmation that officials in Barcelona saw great potential and showed much enthusiasm – but also warned that political, financial and privacy concerns would mean that the road to adoption could be long.

Read more: https://impetus-project.eu

Brief Introduction to the IMPETUS Project

Introducing IMPETUS: watch on YouTube now:

Want to know more? Please contact:

Project Coordinator: Joe Gorman, SINTEF Digital
joe.gorman@sintef.no

Dissemination Manager: K. Harald Drager, TIEMS
khdrager@online.no

Project Coordinator: Pilar De La Torre
delatorre@efus.eu

The IMPETUS Consortium

RESEARCH

- SINTEF
- Institut Mines-Télécom
- University of Nimes
- University of Padova
- National Inter-university Consortium for Informatics

INDUSTRY & SMEs

- SIMAVI
- Thales Nederland
- CINEDIT
- Sixgill
- Insikt intelligence
- UniSMART

NGOs

- Tartu Biotechnology Park
- Croatian Institute for Security Policies
- The International Emergency Management Society

CITIES

- City of Padova
- City of Oslo

For the latest news and updates, please visit us at:
https://impetus-project.eu/

Follow us: