

In collaboration with the Belgian Federal Police



Federale Politie
Police Fédérale

PSCE Conference in Brussels

CONFERENCE REPORT



**Artificial
Intelligence (AI)**



**Climate Change
Emergencies**



**Mission Critical
Applications**

Sponsored by



Table of contents

Executive Summary.....	3
Introduction.....	4
Opening remarks	4
Pitch Elevator #1.....	4
1. Abiom	5
2. 5G-Epicentre	5
3. BroadPort-BroadWay	6
4. Lyfo	6
5. BroadGNSS.....	7
6. Respond-A	7
7. Search&Rescue	8
TOPIC 1: Artificial Intelligence: How can AI enhance First Responders' Situation Awareness?	8
1. <i>The European approach to AI</i> - Yordanka IVANOVA, European Commission (EC) - DG CNECT	8
Background.....	8
Presentation	9
2. <i>Analysing geo-social media using AI algorithms</i> - Bernd RESCH, University of Salzburg	10
3. <i>Augmented connectivity for First Responders in AI-driven UAV missions: an edge-cloud perspective</i> - Leonardo GORATTI, Triagnosys	11
4. <i>Cooperative Digital Solutions for Crisis Management</i> - Mario DROBICS, Austrian Institute of Technology GmbH (AIT)	12
5. <i>Social media usage for Supporting Situational Awareness Systems</i> - Georg AUMAYR, Johanniter Austria	13
PITCH ELEVATOR #2	14
1. Darlene	14
2. Stamina.....	14
3. Faster	15
4. Fire-in	15
5. Ingenious	16
6. iLike	16
TOPIC 2: Climate Change Emergencies: how to improve preparedness?.....	17
1. <i>Union Civil Protection Knowledge Network: how to improve preparedness at EU level</i> - Felix BLOCH, EC - DG ECHO	17
Background.....	17
Presentation	17
2. <i>Recent flooding in Germany: lessons learnt</i> - Uwe KIPPNICH, Bavarian Red Cross	18

3. <i>Preparing for the crisis of tomorrow</i> - Mercedes AGUERRE, French Red Cross	19
4. <i>Public warning: Article 110 - European Electronic Communications Code (EECC)</i> - Joe Lynch, Body of European Regulators for Electronic Communications (BEREC)	20
5. <i>Science and Human factor for Resilient Society (CORE)</i> - Marie-Christine BONNAMOUR, PSCE ...	22
6. <i>Space Applications for improving Emergency Response</i> - Rita RINALDO, European Space Agency (ESA)	23
TOPIC 3: Mission Critical Applications using Broadband Communications: current and future solutions	25
1. <i>Towards an EU-wide interoperable communication system for security</i> - Max BRANDT, EC - DG HOME	25
2. <i>BroadWay: From Solutions prototypes to Pilots implementation</i> - David LUND, PSCE	27
3. National Broadband Applications	29
1. <i>The Netherlands: Introduction and use of mobile applications within the Dutch PPDR organizations</i> - Feiko VERMEULEN, Dutch National Police	29
2. <i>Finland: How 5G, AI and Cloud can enable new public safety services</i> - Kari Junttila, Erillisverkot	30
3. <i>France: Réseau Radio du Futur Programme - priority mobile, secure, high speed, resilient communication system</i> - Renaud MELLIES, French Mol	31
4. <i>Belgium: Towards Mission Critical data in Belgium - Lessons from the past - Visions for the future</i> – Jo DEWAELE, ASTRID	33
4. <i>EPICENTRE: 5G Experimentation Infrastructure hosting Cloud-native Netapps for PPDR</i> - Ioannis MARKOPOULOS, NOVA	35
5. <i>5G critical applications development for First Responders</i> - Drazen RIBAR, AIRBUS	36
6. <i>European Vision for the 6G Network Ecosystem: the voice of the European industry for the development, deployment and evolution of 5G</i> - Mikko UUSITALO, Nokia Bells Lab Finland	37
Funding Opportunities	40
1. <i>Internal Security Fund (ISF)</i> - Arnoud HEERES, EC - DG HOME	40
2. <i>SNS (Smart Networks and Services): the voice of the European industry for the development, deployment and evolution of 6G Smart Networks and Services</i> - David LUND, PSCE	42
PANEL DISCUSSIONS	43
Exhibition Areas	43
PSCE General Assembly & Committees	44
Social event	44

Executive Summary

Public Safety Communication Europe (PSCE) held its 23rd **Conference in Brussels**, on 30th November and 1st December 2021, in collaboration with the Belgian Federal Police, at the *Maison des Associations Internationales*.

Despite a hard Covid-19 context and the implementation of governmental new sanitary measures few days before the conference that forced us to relocate last minute the venue, PSCE decided to maintain the event, gathering around **80 participants** who could meet, discuss on public safety and crisis management, and therefore contribute to the success of its 23rd edition.

“It was very important for us to maintain this conference and offer our members and the public safety community an opportunity to finally meet and discuss in “real life”. Of course, online meetings are useful, but they do not allow for the same degree of interaction and sharing of knowledge, which are key elements in our conferences” stated Marie-Christine Bonnamour, Secretary-General of PSCE.

The scale, frequency and unpredictability of crises seem to be increasing and the resulting consequences are becoming more and more dramatic. All actors involved in such crises, from public authorities to solution providers, are concerned and constantly seek to better prevent and minimize their impact.

Three **topical issues** were addressed during the conference: *“Artificial Intelligence (AI): how to enhance First Responders’ Situational Awareness”*; *“Climate Change Emergency: how to improve preparedness”*; *“Mission Critical Applications using broadband communication: current and future solutions”*.

The conference was attended by a variety of **EU officials** and experts (DG CNECT, DG ECHO, DG HOME, ESA) who provided valuable policy insights relevant to the themes and topics addressed. In addition, around 13 projects were presented, 10 exhibitors holding a booth presented their solutions and products, including our 4 sponsors, namely **Abiom, Airbus – Defence & Space, Lyfo, Motorola Solutions**, all contributing to create a clustering of exchange for innovative solutions in public safety.

The debates triggered by the topics at PSCE Conference will certainly contribute to improving the efficiency of public safety operations and PSCE is happy to be part of this drive.

All conference documents and the recording are made available to conference participants and to PSCE Institutional Members, as well as the conference report and overview video.

Introduction

The conference was kicked-off with an inspiring and warm introduction by **Monika Büscher, PSCE President**.



"It's a truly outstanding programme PSCE at its best; we have 3 highly topical sessions with high profile speakers, developing the deep dialogue between practitioners, industry, policy and research, that PSCE is famous for".

Opening remarks

The introduction was followed by the short and rewarding opening remarks of Etienne Lezaack, System Architect for Police Information and ICT, on behalf the **Belgian Federal Police**.

"It was foreseen that I would welcome you in our premises, at the Federal Police Centre, but unfortunately, last week the covid restrictions became so strict that all the events in our premises were cancelled.

So, I have to congratulate the PSCE team to have found a solution in a so short period: really, you have a big resilience, it's incredible".




Pitch Elevator #1

Seven Industry entities and EU projects that provide solutions in the public safety and crisis management domains were presented before the opening of the first topic, namely **Abiom, 5-G Epicentre, BroadPort-BroadWay, Lyfo, BroadGNSS, Respond-A, Search&Rescue**.

1. Abiom

ABIOM CS member of Mission Critical Group

- Distributor in the BeNeLux for Public Safety and industry with products as :
Phonak, Sepura, Bittium and Lifeline



**Bittium
Tough Mobile 2**

- Unbreakable chain of security
- Rugged
- Fully controlled by MDM
- long lifespan



- Lifeline, Your portable radio in app format

MAXIMIZING MOBILITY, CREATING CONNECTIVITY

ABIOM

www.abiom.be

Abiom is the leading and innovative player in the Benelux with respect to the development, supply, production and service of high-quality mission and business critical communication solutions. Also, Abiom specializes in vehicle signalling systems for professional work environments. Our customers continuously challenge us since they must be able to trust in flawless communication under all circumstances, during a mission or a deployment. Abiom is the exclusive distributor in the Benelux of high-end communication solutions from a wide range of renowned brands, such as Sepura (TETRA Radios and accessories), Phonak (hearing protection and covert communication solutions), TPL (Paging terminals). We also offer a portfolio of in-house tailor-made solutions for different use cases.

2. 5G-Epicentre

5G ExPerimentation Infrastructure hosting Cloud-native Netapps for public proTection and disaster RELief Objectives & Benefits

5G PPDR

End-to-end 5G experimentation platform specifically tailored to the needs of the public safety and emergency response market players.

'5G Experiments as a Service' model, which will enable developers and SMEs to experiment with PPDR applications.

Facilitate automation, continuous deployment and multi-access edge computing functions, to reduce service creation time and time-to-market for 5G PPDR solutions.

- Containerization of the 5GCore**
Enhancement to the performance of the core network, superior experimentation infrastructure and K8s support for automated operations.
- Lightweight virtualization toward MEC**
Faster instantiation, low resource utilization, platform independence and smaller footprint, delivering significant boost to mobility.
- Flexible allocation among edge and centralized core**
maximize amount of resources reliably executed close to the first responders, optimize the combined Cloud and MEC infrastructure.
- Development & sharing of CNFs via open repository**
Facilitate collaborative development and lead to ground-breaking innovation along with higher-quality services for PPDR agencies.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 101016521

<https://www.5gepicentre.eu/>

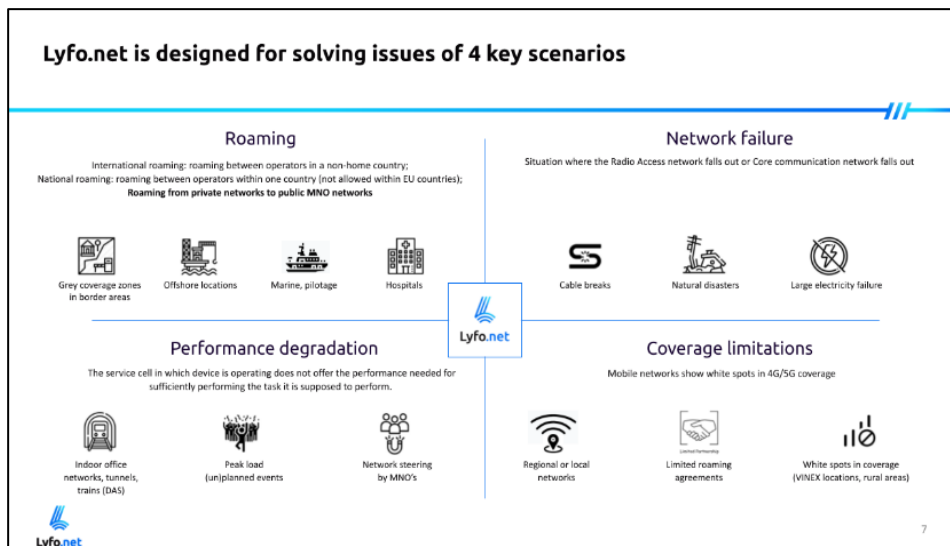
5G-EPICENTRE (5G Experimentation Infrastructure Hosting Cloud-Native Netapps) aims to lower barriers to 5G adoption and market entry for European SMEs to conduct rigorous experimentation of their products and applications aimed at public safety market, through the provision of an open, federated, end-to-end experimentation facility.

3. BroadPort-BroadWay

BroadPort consortium led by FREQUENTIS is currently in Phase 3 of the Horizon 2020 Project “BroadWay”. In Pilot Phase the consortium builds a live system of a pan-European broadband communication system for trials. The ambition of the BroadWay project is to achieve operational mobility for public safety responders across Europe by linking national mission-critical mobile broadband networks to act as one. This will allow pan-European national mobility and the communication between first responders, providing the highest levels of security and reliability across Europe, at any time, regardless of their location. European first responders will benefit from new mission-critical communication capabilities, enabling closer collaboration and saving lives when disasters hit.

<https://www.broadway-info.eu/consortium-b-frequentis/>.

4. Lyfo



www.lyfo.com

We revolutionize Mobile connectivity in poor or no coverage scenarios by switching between Mobile NextGen Networks in seconds, guaranteeing “Always Connected”! The missing link between First Responders and Mobile Operators is our patent pending Lyfo.net Network Selection Technology. Keeping you connected is our mission!

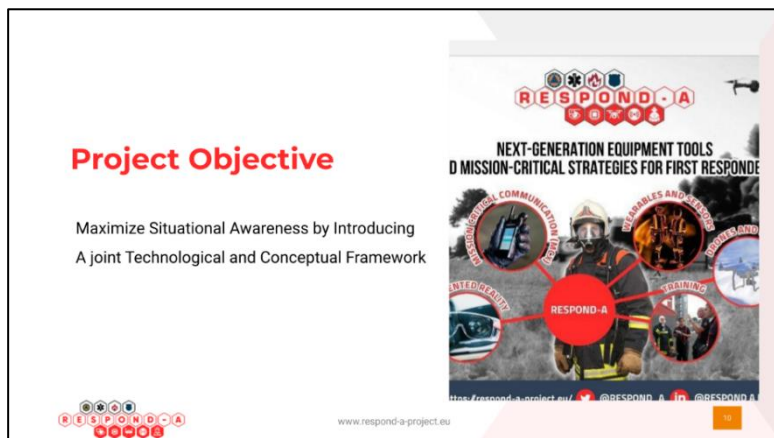
5. BroadGNSS



The BroadGNSS project will take the first procurement steps exploit the distinguishing features of EGNOS and Galileo Signals and operational advantages in downstream public safety applications, to improve the services of Public Safety and Disaster relief organisation's (PPDR's) to Europe's citizens. The primary goal of this project is: Pre-Commercial Procurement (PCP) of innovation activity to develop Deployed Applications and Monitoring of Critical Mobile Broadband Communication Infrastructure and Assets for PPDR. This project implements a Pre-Commercial Procurement (PCP) with the purpose to realise innovative solutions for a number of application areas to fulfil capability needs regarding the accuracy, reliability, assurance and cost of positioning systems.

<https://www.broadgnss-info.eu/>

6. Respond-A

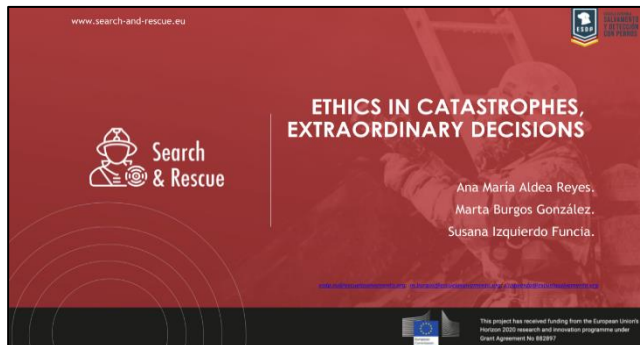


<https://respond-a-project.eu/>

RESPOND-A aims at developing holistic and easy-to-use solutions for First Responders by bringing together the complementary strengths of its Investigators in 5G wireless

communications, Augmented and Virtual Reality, autonomous robot and unmanned aerial vehicle coordination, intelligent wearable sensors and smart monitoring, geo-visual analytics and immersive geospatial data analysis, passive and active localization and tracking, and interactive multi-view 360o video streaming.

7. Search&Rescue



The key objective of S&R is to develop and promote the underlying framework (interoperability among systems and equipment, training and awareness) so that responders at all levels of command have access, familiarise and evaluate how to deploy innovative solutions. The major challenge addressed is to link approaches, technical solutions, procedures, standards, for the protection of the European citizen thus allowing for a faster and more appropriate response to natural, technological and man-made threats in EU countries and if needed abroad.

<https://search-and-rescue.eu/>

TOPIC 1: Artificial Intelligence: How can AI enhance First Responders' Situation Awareness?

1. The European approach to AI - Yordanka IVANOVA, European Commission (EC) - DG CNECT



Yordanka Ivanova is a Legal and Policy Officer in the European Commission (DG CNECT, A2) in the unit responsible for Artificial Intelligence Policy Development and Coordination. She started her career in the European Commission in 2011 working as a policy officer in DG ECHO in the area of disaster prevention and civil protection. Outside the Commission, Yordanka has experience as a researcher and attorney-at-law, advising companies on EU regulations, including in the area of data protection, digital services, financial services, cybersecurity and copyright.

Background

The **European approach to artificial intelligence (AI)** aims to build a resilient Europe for the Digital Decade where people and businesses can enjoy the benefits of AI. It focuses on 2 areas: excellence in AI and trustworthy AI.

To help further define its vision for AI, the European Commission developed an [AI strategy](#) to go hand in hand with the European approach to AI. The AI strategy proposed measures to streamline research, as well as policy options for AI regulation, which fed into work on the AI package. The Commission published its AI package in April 2021, proposing new rules and actions to turn Europe into the global hub for trustworthy AI.

This package consisted of (i) the [Coordinated Plan with Member States: 2021 update](#) and (ii) a [Proposal for an AI Regulation](#) laying down harmonised rules for the EU (Artificial Intelligence Act).

Presentation

Ms. Ivanova introduced the **pros and cons of AI**, including the risks related to the safety and fundamental rights of consumers and users, reminding chronologically all the key initiatives of the EC to make rules on it (European Strategy on AI, Guidelines for Trustworthy AI, First Coordinated Plan on AI, White Paper on AI, and AI package).

After considering the **Coordinated Plan on AI** (2021) as a joint commitment between the Commission and Member States (MS) to make Europe maximise its AI potential to compete globally, the **Proposal for a Regulation on AI** as a horizontal, uniformising, innovation-friendly, risk-based legislation, and the **AI** as *“a software that is developed with one or more of the techniques and approaches listed in Annex 1 and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with”*, Ms. Ivanova entered into more details on the risk-based approach to regulation.

In a law and law enforcement perspective, Ms. Ivanova presented the four possible (and not exclusive) **distinct risks related to AI**: minimal (or no risk), specific transparency obligations, high risk, unacceptable risk.

However, most AI systems are not high-risk:

- the **minimal risks** are related to possible voluntary codes of conduct for AI with specific transparency requirements and the (new) specific transparency obligations are mostly to notify human that (i) they are interacting with an AI system or (ii) emotional recognition or biometric categorisation systems are applied to them.
- about the **high-risk** AI systems, they concern (i) AI safety components of regulated products like medical devices or machinery and (ii) certain AI systems Ms. Ivanova detailed, such as “biometric identification and categorisation of natural persons”, “law enforcement”, “migration, asylum and border control management”, among other fields. Not forgetting the requirements for high-risk AI and the obligations of operators of high-risk AI systems.
- concerning the **unacceptable risks**, Ms. Ivanova mentioned examples of AI that contradict EU values and thus are prohibited (such a subliminal manipulation and exploitation of children or mentally disabled persons resulting in physical or psychological harm, general purpose social scoring, remote biometric identification (RBI) for law enforcement in publicly accessible spaces), the five cumulative conditions for the prohibition of RBI, and the exceptions of authorisation.

Ms. Ivanova finished with the AI Package's **next steps**: (i) co-legislation with the European Parliament and the Council to agree on a regulation, (ii) transitional period of two years before the agreed regulation becomes directly applicable, (iii) in parallel, harmonised standards of CEN/CENELEC to be ready and support the implementation of the new rules and conformity assessment procedures.

2. Analysing geo-social media using AI algorithms - Bernd RESCH, University of Salzburg



Bernd Resch is an Associate Professor at University of Salzburg's Department of Geoinformatics - Z_GIS and a Visiting Scholar at Harvard University (USA). Bernd Resch did his PhD in the area of "Live Geography" (real-time monitoring of environmental geo-processes) together with University of Salzburg and MIT. His research interest revolves around understanding cities as complex systems through analysing a variety of digital data sources, focusing on developing machine learning algorithms to analyse human-generated data like social media posts and physiological measurements from wearable sensors. The findings are relevant to a number of fields including urban research, disaster management, epidemiology, and others.

Mr. Resch started his analysis on *supporting Crisis Management and Prevention with Geo-social Analytics* taking a quick look at the cons of **current approaches** and the pros of the crowdsourced data that lead to the following assessment: uncertainty remains, and the information is unstructured and non-standardised.

With **crisis examples** such as summer German floods (2021), massive refugees border crossing from Budapest to Austria (2015), Beirut's Port destruction (2020), Mr. Resch showed how it is possible to know, from Twitter or Instagram social media raw data, where the relevant social media posts cluster, given that such posts are fast, geo-located and multimedia information.

Mr. Resch highlighted the **Napa Valley earthquake (USA, 2014)** related to Twitter activity: (i) the *tweets* per hour around the day of the earthquake are regular and stable until they double when the earthquake occurs while the *tweets* per minute the day of the earthquake are the same until they almost increase tenfold when the occurrence of the earthquake; (ii) there is a positive correlation between the intensity of the earthquake footprint and the intensity of *tweets* posting, when considering the areas up to 100km in all the directions. We observe the same phenomenon with the Hurricane Harvey (USA, 2017) or with the Covid-19 situation and the US related tweets: for the latter, when the 24-25/01/2020 the World Health Organisation (WHO) declares a "potential pandemic", tweets increased to 20 000; when WHO declares two weeks later the effective pandemic, tweets skyrocketed to 100 000 in two more weeks.

Geo-social Media Analytics are worldwide available, model the spatial spread of crisis situations, allow continuous data stream and real-time situation reporting, are intuitive, portable from a use case and a geographic region to another and can be simply integrated into disaster management processes.

While the geospatial analysis suffers uncertainties in data-rich environments, the "**geoAI**" offers new possibilities to filter, analyse and understand data, to detect (unanticipated)

patterns, to model with lower efforts, to go beyond an “*exclusively-geo*” analysis with a multi-modal one.

3. Augmented connectivity for First Responders in AI-driven UAV missions: an edge-cloud perspective - Leonardo GORATTI, Triagnosys



Leonardo Goratti has a PhD in Telecommunications awarded by the University of Oulu, in Finland. He is a senior systems engineer with seventeen years of experience in the ICT domain and matured in distinguished institutions and large industries. He possesses in-depth understanding of 5G technology (3GPP Rel.15 through 17), as well as of beyond 5G and 6G technological foundations. Leonardo Goratti is knowledgeable in cloud technology applied to the telecom sector availing software-defined networking (SDN) and network function virtualisation (NFV) technologies.

Mr. Goratti introduced his talk with a short analysis: first responders operate in extreme conditions and need cutting-edge technologies. He took the example of the EU-funded project **Respond-A** and its *Common Operating Picture* (triage, toxic detection, 360° camera images), that focuses its research on the first responders’ communication in emergency scenarios, to analyse some issues to tackle and the related proposed solutions.

Mr. Goratti presented an example of scenario, a Respond-A use case, a **UAV exploration** mission in the Port of Valencia, before the first responders arrive to the fire area.

On the first hand, the **problems** to tackle are related to (i) the offline path computation based on the information discovered from a georeferenced map, (ii) the online obstacle detection and avoidance, and points of interest recognition, (iii) process of camera images.

On the other hand, the proposed **solution** is the *Particle Swarm Optimisation (PSO)* method that is a computational intelligence AI which generates and updates paths (but it suffers problems of local minima and constraints with drone use).

Mr. Goratti showed us the **model accuracy** from Google Earth screenshot to *Python Overpass Turbo* model and few examples of 2D path computations, before comparing the 2D and 3D models. He finished with the presentation of an UAV flight plan with a *Pixhawk* drone autopilot.

4. Cooperative Digital Solutions for Crisis Management - Mario DROBICS, Austrian Institute of Technology GmbH (AIT)



Mario Drobics is Head of Competence Unit for Cooperative Digital Technologies at the AIT Austrian Institute of Technology GmbH. He received his PhD in applied mathematics in 2005 at the Johannes Kepler University Linz in Austria. Since 2007 he is working in the Centre for Digital Safety & Security at AIT. His research addresses various aspects of digitalization, including security, IoT, and data analytics, focusing on the application in different domains like public safety, manufacturing, and health. Dr Drobics is Head of a working group on IoT Security at OVE-GIT, member of the AIOTI Alliance and member of the national ISO/IEC JTC1-SG41 (IoT) working group.

Mario Drobics started presenting the **AIT's Centre for Digital Safety & Security** that focuses on secure and resilient digital systems for the digitalisation of the industry, economy and society, and more specifically domains such as AI, Cybersecurity for critical infrastructures, wireless networks (5G), protection of democracy, among others.

He defined the four actions on data that enable the **"Cooperative Digital Technologies"**: collect, exchange, understand, share; respectively, data acquisition and edge computing, federated data distribution and workflows, data analytics and prediction, and knowledge sharing.

He also described the **data utilisation**, among other things the IoT signal level, the edge local level or the data spaces domain level and stated that the Edge computing (or Edge AI) is more profitable than the dominant cloud computing model (following the EC assessment).

Mr. Drobics presented then **four use cases**, namely Public Safety Hub (PSH), Crowd Tasker, Social Media Analysis, Remote Sensing, as relevant examples of interoperability solutions:

- concerning the **PSH**, there was a need of enabling synergetic sharing of data with various kinds of organisations, therefore a trustworthy and resilient information exchange: on interoperability solutions, tactical information, warnings and alerts:

- about **Crowd Tasker**, the aim was to integrate volunteers in public safety actions, which involved collecting and distributing information, delegating tasks to volunteers based on their geolocation, skills, demand. So, between professionals and volunteers were set up a web-based admin interface and a mobile app for volunteers, to ensure crowd tasking, alerting and sourcing.

- on **Social Media Analysis**, it was all about improving situational awareness, using a combination of two Neurolinguistic Programming techniques (topic models and term frequency-inverse document frequency algorithm (TF-IDF)); Mr. Drobics gave examples of the event detection with FIS Nightrace 2020 in Schladming event and the sentiment mapping with the Covid-19 impact.

- regarding the **Remote Sensing**, the purpose was the analysis of earth observation satellite data. Examples were given on vegetation remote sensing analysis with an automated context-based monitoring of small-to-large scale spatiotemporal features in a selected scenery, and the integration of such remote sensing to a *Ground truth validation*.

Mr. Drobits finished with the presentation of **AIT Climate Services**: climate-resilient, economic and sustainable planning and support of urban infrastructure projects and measures for city planners, projects developers and infrastructure owners.

5. Social media usage for Supporting Situational Awareness Systems - Georg AUMAYR, Johanniter Austria



Georg Aumayr studied journalism and communication science in Vienna. He is Research Officer of Johanniter International and since 2021 Research Director of Johanniter-Unfall-Hilfe in Austria. Before that, he was a Research Assistant at the Research Institute of the Red Cross and worked in the ambulance service for many years. Mr. Aumayr's research spans the security area, including the protection of the population and emergency services.

Mr. Aumayr started with the review of the **Standard Situation** when facing disasters and critical situations: (i) the need of knowing forces and resources available, location and movement, and time, (ii) the reception of data from assessment teams, (iii) the gathering of information with a situation report. To sum up, the need to get information about its own situation and about others' (victims or enemies).

He reviewed the expectations from **social media data** as well as the latest support tools Johanniter Austria tested: Social Media Grabber, Sentiment Analysis, Automated Picture Processing, Google Analytics. Some results are that (i) keywords are problematic, (ii) data sources are limited, (iii) fake news become more and more a problem; so, respectively, (i) content structure, (ii) availability, and (iii) trust are social media requirements that cannot be fully ensured.

M. Aumayr mentioned some **successful experiences**, namely (i) HUMAN+ and (ii) METICOS project that respectively (i) watched refugees moving by Social Media Analysis and extrapolated potential routes and headcount of refugees' streams, and (ii) conducted an Acceptance analysis by social media data of border control systems. HUMAN+ allowed a good understanding of the movements and motivation of people while METICOS supported the detection of keywords by an abstract ontology.

He finished presenting some current actions of Johanniter Austria, in terms of **Keywords identification**: automatic filtering of filling words, semi-automated social network analysis, code scheme for related terms, iterative screening of keywords and ontology clouds with translations, separation of content from sentiment; with an example of Social Networks Analysis (SNA). The major finding was about **intersectionality**: gender and diversity have a great influence on the use of social media, communication habits, reflection of events in public and wording; background information and relational perception of data are a challenge but also a requirement to support the use of social media as a source for situational awareness support.

PITCH ELEVATOR #2

Six Industry entities and EU projects that provide solutions in the public safety and crisis management domains were presented before the opening of the second topic, namely **Darlene, Stamina, Faster, Fire-in, Ingenious, iLike**.

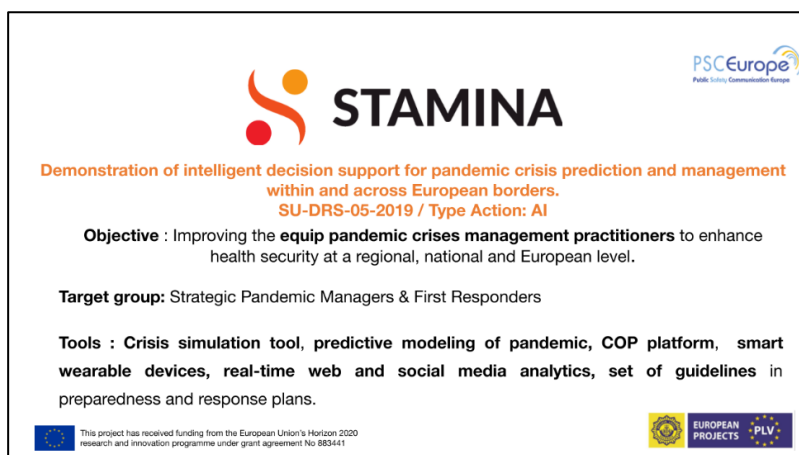
1. Darlene



<https://www.darleneproject.eu/>

DARLENE aims to unlock the capacity to rapidly foster visual understanding of complex real-world scenes in public safety situations by investigating how cutting-edge augmented reality (AR) technology can be deployed to help Law Enforcement Agencies and first responders make more informed and rapid decisions especially in situations where time is of the essence. The project develops innovative Augmented Reality tools that aim to improve situational awareness when responding to criminal and terrorist activities.

2. Stamina



<https://stamina-project.eu/>

STAMINA helps to overcome serious cross-border public health threats by providing improved decision-making technology to pandemic crisis management practitioners at a regional, national and European level. Its solution provides national planners, regional crisis management agencies, first responders and citizens with new tools as well as a clear guide to how they can be used in line with international standards and legislation.

3. Faster



<https://www.faster-project.eu/>

FASTER (First responder Advanced technologies for Safe and efficient Emergency Response) aims at addressing the challenges associated with the protection of first responders in hazardous environments, while at the same time enhancing their capabilities in terms of situational awareness and communication. To do so, FASTER will develop a set of important supporting technologies such as UAVs and UGVs, resilient communications, technologies for companion K9 units and mini-UAVs and AR tools for improved situational awareness.

4. Fire-in

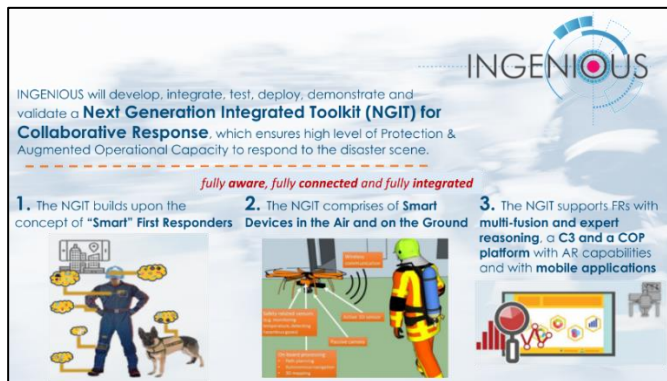


<https://fire-in.eu/>

<http://demo.fire-in.eu/>

The main objective of FIRE-IN, the first European Fire & Rescue Network, is to improve the national and European Fire & Rescue service capabilities, develop process by fostering innovation and promote cutting edge solutions to address identified operational needs. The main tool develop for the project is the e-FIRE-IN platform, where stakeholders can connect to the Fire and Rescue community, share and search project results or invite peers to collaborate.

5. Ingenious



<https://ingenious-first-responders.eu/>

INGENIOUS aims to assist First Responders be more effective and save more lives during natural and manmade disasters and crises by exploiting novel technologies. INGENIOUS is developing, integrating, testing and validating a Next Generation Integrated Toolkit (NGIT) for Collaborative Response, which ensures high level of Protection and Augmented Operational Capacity to respond to the disaster scene.

6. iLike



<https://www.kiras.at/en/financed-proposals/detail/ilike>

iLike is an intelligent situation information portal for the collection and processing of relevant information from publicly available data sources designed to support emergency organizations in disaster management using an innovative and user-centred approach. The goal is to design an intelligent situation information portal that enables the integration of publicly available information sources and channels to foster disaster mission management. The primary objective is to ensure the availability of data, to collect and analyse it, and to extract relevant information. The project aims to create a prototype and collect requirements and lessons learnt for future developments.

TOPIC 2: Climate Change Emergencies: how to improve preparedness?

1. Union Civil Protection Knowledge Network: how to improve preparedness at EU level - Felix BLOCH, EC - DG ECHO



Felix Bloch is Head of Unit for “Knowledge Network and Evidence-Based Policy” at the European Commission (DG ECHO). In 2012 he became personal assistant to a Deputy Director General in DG AGRI from where he moved in 2015 to DG ECHO. At DG ECHO he was the Assistant of the Director-General (Monique Pariat). In 2017 he joined the Cabinet of the Commissioner for Humanitarian Aid and Crisis Management, Christos Stylianides. At the Cabinet he was in charge of the legislative initiative to strengthen the Union Civil Protection Mechanism (“rescEU”).

Background

Natural and human-induced disasters are increasing in intensity and complexity, claiming lives, destroying livelihoods, and causing substantial damage to individuals and societies. A plethora of initiatives, distinct financial instruments, projects, programmes, organisations, networks and communities operating in parallel result in fragmentation of resources, knowledge and expertise. In the face of the increasing complexity of challenges the EU is facing, it is imperative to reduce this fragmentation and make the elements of this landscape better match and contribute to each other’s success. A “network of networks” and a convenor for the sector, the **Union Civil Protection Knowledge Network (UCPKN)** will boost the EU civil protection and disaster management system to enable it to tackle existing and emerging challenges.

Presentation

Mr. Bloch started with reviewing the **Union Civil Protection Mechanism (UCPM)**: its role (“encourage cooperation between Member States (MS) for preventing and protecting against natural or man-made disasters”¹) and its members (all EU MS and 6 participating States).

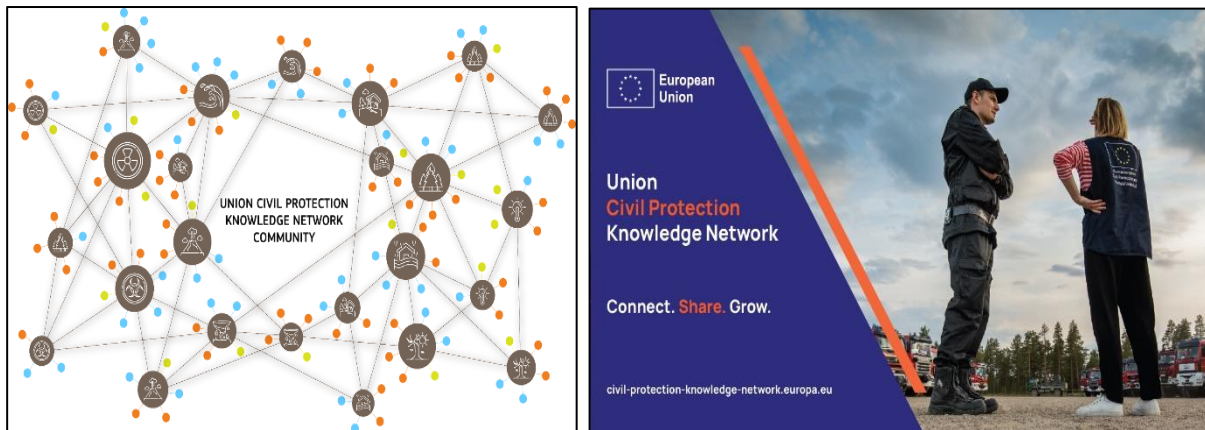
He introduced the UCPKN (launched on *Knowledge Network Day* one week later, on 7th of December 2021) with the words of Commissioner Janez Lenarčič (2021): “*We know that **resilience depends on preparedness. And preparedness depends on knowledge** – and tools that deliver that knowledge to those who need it. This is the role of the Union Civil Protection Knowledge Network*”.

Mr. Bloch continued with the presentation of the **UCPKN**: **(i)** a knowledge broker, partnership facilitator and innovation catalyst, **(ii)** based on the Capacity Development and Science Pillars, respectively to connect, promote and strengthen capacity development initiatives, and to

¹ Article 196, TFEU

bring together academia, practitioners and decision-makers for multi-disciplinary, cross-sectoral and cross-border cooperation, (iii) integrating UCPM Training Programme, Awareness-raising activities, UCPM Lessons Learnt Programme, Exchange of Civil Protection Experts, Community engagement, Scientific advice and innovation, Civil protection exercises, Partnerships facilitation opportunities, Thematic workshops and conferences.

Mr. Bloch ended with the **benefits** of such Knowledge Network, for Policy makers, Practitioners and Researchers (among other things and respectively: stronger evidence to support decision-making; easy access to guides, toolkits, good practices and lessons learnt; stronger ties between science and disaster management).



2. Recent flooding in Germany: lessons learnt - Uwe KIPPNICH, Bavarian Red Cross



Uwe Kippnich is the Coordinator Security Research at the Bavarian Red Cross HQ in Munich and its representative for the AIFER (Artificial Intelligence for Emergency Response) project. He is a high-level trained expert for the EU Civil Protection Mechanism. He was involved in the COVID-19 crisis management and as a commander active e.g., from a medical task force during the flooding in July 2021 in Germany. He is a member of the PSCE – Board and its vice president.

Mr. Kippnich gave some insights on the AIFER project with a focus on how **drone images** can help the emergency response in disaster areas, including sharing his experiences regarding the crisis management during the mass flooding in Germany in July 2021 with a focus on the use of satellite and drone images and their usefulness for the assessment for commanders, control rooms and command posts onsite the disaster scene.

He shared with us the **prediction** of severe rainfall and the related warning few days before the flooding, and various **images**: air images from the Federal Republic of Germany's research centre for aeronautics and space's (DLR) helicopter; picture of the Base of Operations (BoO), integrated control centres and Centre for Satellite Based Crisis Information (ZKI); pictures and

process of the on-site assessment in the affected areas close to the river Ahr; pre- and post-disaster maps.

Mr. Kippnich also presented the **AIFER** project, part of the long-time partnership with the DLR – ZKI cooperation, with pictures of UAV flights in Altenburg flooded region. He explained the **AIFER next generation rapid mapping**: Triggering of Data Acquisition and Mapping, Multimodal Data Acquisition, Innovative Analysis Techniques, New ways of Dissemination, Visualisation and User Interaction. The AIFER first results were presented at the ESA space2connect 2021 conference, last 11 October 2021.

Mr. Kippnich concluded with the **lessons learnt**:

- In times of crisis, knowing the right people is the key (BRK Security Research's wide network)
- The easiest solution tends to be the best one
- Contents from research projects were useful
- Successful first direct cooperation of assessment teams on site and from satellite centres (ZKI/DLR)
- The User acceptance is still a challenge

3. *Preparing for the crisis of tomorrow* - Mercedes AGUERRE, French Red Cross



Mercedes Aguerre is Coordinator of Disaster Risk Reduction and Health projects at the Emergency and Risk Management Department at the French Red Cross. She is responsible for the development of national and European projects in the field of Disaster Risk Reduction (DDR), Climate Change Adaptation (CCA) and Health. She has worked in different contexts such as Guatemala, Afghanistan, Haiti, Niger, Ethiopia Ecuador and Peru, conducting and supporting Disaster Risk Reduction programs.

Ms. Aguerre started by a presentation of the **French Red Cross (FRC)** and its 65 000 volunteers and 16 000 employees: **(i)** its aim (protect and support vulnerable people), **(ii)** its missions in the frame of 2030 Strategy (prevent and educate, protect, and support the recovery of social connections), **(iii)** its main actions (emergency and rescue operations, social action, health and medico-social support, capacity building, international operations).

She also underlined the **need to be prepared**, given the changes and increases in the type, scale and intensity of disasters and emergency situations. Not only Climate change is a risk; other interconnected risks will affect us somehow: acceleration of technological and economic disruption that accentuates inequalities and gaps, intensification of natural, industrial and health risks, and demographic issues and policies that lead to violence.

To the question “**how to be prepared for the crisis of tomorrow**”, Ms. Aguerre mentioned **three pillars**: (i) rely on the population, (ii) open to new forms of engagements, (iii) plan for the future; in other words, collaborate, innovate and adapt.

- about **relying on the population**, Ms. Aguerre mentioned the French *Law n°2004-811 of the 13 August 2004 on the modernisation of civil security* that involves, practically, the public to

civil security. She gave another example of collaboration with “*la caravane d’été*” (“the summer van”), an initiative that aims at taking the road and meeting as many people as possible to introduce them to life-saving actions, risk-reduction and prevention of accidents.

- about **opening to new forms of engagements**, given the new complex and converging crisis, the French Red Cross adapts its procedures, recruitment frameworks and training to increase its capacity of action, to improve its influence and to better respond the needs. For instance, new volunteer commitments were elaborated: spontaneous ones (by signing convention with municipality during the crisis), one-day ones (pre-established, by signing the FRC chart), community relay (to bring citizens closer to local action and decision-making).

- about **planning for the future**, the FRC adopted new preparedness and response mechanisms (due to new emerging risks), and equipment. Two examples were given: Heatwaves preparedness and Multi-site and multi-risks events (MERCI project). Since 2003 and the intense drought France suffered, emergency interventions and preparedness measures increased and were set up as a response mechanism; the FRC followed the national initiative and developed its own Heatwave Plan. Regarding the MERCI project, it aimed at increasing resilience in large European urban areas facing major accidents, by improving the coordination between the volunteer organisations and public authorities.

Ms. Aguerre concluded with a review of the FRC at the **international level**: being part of the Federation of Red Cross and Red Crescent Societies (IFRC) and benefiting from the Regional Intervention Platforms (PIR) in Indian Ocean, in the Caribbean and in the South Pacific, the FRC conducts projects that increase resilience, disaster risk management, awareness and capacity building.

4. Public warning: Article 110 - European Electronic Communications Code (EECC) - Joe Lynch, Body of European Regulators for Electronic Communications (BEREC)



Joe is passionate about radio science and propagation phenomena in wired and wireless communications systems. He holds a Master of Science degree in Experimental Physics from Maynooth University, an Executive MBA degree from University College Dublin, and a Diploma in Digital and Marketing Strategy from the Irish Management Institute where he was student of the year (2017). He has 15 year’s communications experience in various positions in regulation and international relations, including as a delegate for Ireland at the ITU Regional Radio Conference held in Geneva in two sessions (2004 and 2006)

Mr. Lynch started by introducing the **Body of European Regulators for Electronic Communications (BEREC)**: established by Regulation (EU) 2018/1991 of the European Parliament (EP) and of the Council of 11 December 2018, it is composed of the Heads or nominated high-level representatives of the National Regulatory Authorities (NRAs) of the EU Members States (MS), and it is also open to the participation of Regulatory Authorities of third countries with primary responsibility in the field of electronic communications, where those third countries have entered into agreements with the European Union to that effect. BEREC aims at fostering the independent, consistent and high-quality regulation of digital markets for the benefit of Europe and its citizens.

Then, he presented the **Article 110 of the European Electronic Communication Code (EECC)**:
*§1. By 21 June 2022, Member States shall ensure that, when public warning systems regarding imminent or developing major emergencies and disasters are in place, public warnings are transmitted **by providers of mobile number-based interpersonal communications services to the end-users concerned**.*

*§2. Notwithstanding paragraph 1, Member States may determine that public warnings be transmitted through publicly available electronic communications services other than those referred to in paragraph 1, and other than broadcasting services, or through a mobile application relying on an internet access service, provided that the effectiveness of the public warning system is **equivalent in terms of coverage and capacity to reach end-users**, including those only **temporarily present in the area concerned**, taking utmost account of BEREC guidelines. Public warnings **shall be easy for end-users to receive**.*

By 21 June 2020, and after consulting the authorities in charge of PSAPs, BEREC shall publish guidelines on how to assess whether the effectiveness of public warning systems under this paragraph is equivalent to the effectiveness of those under paragraph 1.

Mr. Lynch then gave a review of the **Guidelines on Public Warning Systems (PWS Guidelines)** that assume Cell Broadcast (CB) and Location Based SMS (LB-SMS) are 110(1) and that Internet Access Services (IAS-PWS) applications are 110(2) systems, and that leveraged early engagement (28 responses to general NRA surveys, 24 responses to detailed NRA surveys, 15 stakeholder submissions, 20 responses to draft Guidelines). He presented the *3-step approach* methodology, from a preliminary step of MS identifying compliant 110(1) systems: (i) Benchmark creation (assessing identified 110(1)-PWS' performance against factors), (ii) 110(2)-PWS' assessment (of performance against factors), (iii) Equivalence assessment (comparing 110(2)-PWS' performance against the benchmark).

Mr. Lynch concluded presenting some **key points** about the PWS Guidelines, namely the **Assessment factors** and the **Comparative Assessment**. The first key point focuses on the non-exhaustive list of factors "toolbox" about the coverage or the capacity to reach concerned end-users (whose "geographical targeting", "scalability" and "supporting visiting end-users" factors are addressed by BEREC's interpretative of *Code: All ECS-PWS*). The second key point focuses on factor-by-factor comparisons to ensure an overall assessment of coverage and/or ability to reach concerned end-users in the round.

5. Science and Human factor for Resilient Society (CORE) - Marie-Christine BONNAMOUR,
PSCE






Marie-Christine Bonnamour is specialised in European law and European affairs. She has been working in various EU projects, being responsible for dissemination and communication activities. She has been also working for the medical profession and the police administration at EU level during the last 15 years and is the Secretary General of PSCE since 2009. She is also Auditor at the French National Institute of High Studies on Security and Justice. As Secretary General, she is managing and coordinating PSCE involvement in the EU funded projects

Ms. Bonnamour started presenting the EU-funded project **CORE** (sScience and human factor for Resilient society), that will be conducted from the 01/09/2021 to the 31/08/2024, with 19 partners from 11 countries that form a multi-disciplinary consortium.

She gave a view on the **objectives** of CORE: **(i)** define common metrics with respect to the different natural and man-made disaster scenarios, and how to measure, control and mitigate the impact on the populations, **(ii)** identify and use best practice and knowledge / learning from certain countries, such as Japan which experienced high levels of seismic, volcanic and tsunami risks but where risk awareness is high, **(iii)** devote great attention to education in schools and vulnerable groups: disabled, elderly, poor, as well as women and children. In other words, to develop a harmonized vision of crisis management awareness and capability through a transdisciplinary collaboration involving the environmental science and social science communities.

Ms. Bonnamour also presented the CORE **methodology** and its five **Building Blocks** that will ensure to cover the whole of disaster management cycle, as they encompass: prevention; preparedness; emergency management; response; recovery. The main **outputs** will be CORE (i) policy recommendations, (ii) ethical recommendations, (iii) App in collaboration with schools, as young people will become the next “*prevention sentinels*”.

CORE Structure		Description
	3 CORE's Goals	1 – Measure
		2 – Control
		3 – Mitigate

 3 CORE's Pillars	1 – Hard science 2 – Social Science 3 – Societal Acceptance
5 CORE's Building blocks 	1 – Safety Culture 2 – Social media support and threats to safety culture and community resilience 3 – Disaster scenarios, human behaviour, and disaster community identity as resilience factor 4 – Cascading effects 5 – Governance
 6 CORE's Test cases	1 – Earthquake 2 – Terrorist Attack 3 – Industrial Accident 4 – Flash Flood 5 – Tsunami 6 – Covid-19

6. Space Applications for improving Emergency Response - Rita RINALDO, European Space Agency (ESA)



Rita Rinaldo has obtained her master's degree in Telecommunications Engineering (summa cum laude) from the University of Bologna in March 2000. In May 2005 she has received her PhD and in 2014 her MBA. Since February 2001 she has been with the European Space Agency, taking up different positions with the Technical Directorate first and then with the Telecommunications and Integrated Applications Directorate. She is currently in charge of the Partner-Led and Thematic Initiative Section in the Integrated and Telecommunications-related Applications Department, where she is responsible for the initiation and management of space-based applications projects in the relevant vertical sectors.

Ms. Rinaldo started reviewing the variety of domains **for space applications**, such as safety and security, environment and wildlife, energy and utilities, health and social care, transport and logistics, and agriculture, forestry and fishing (that constitute more than 600 activities from 2016 to 2021 for ESA). Also, the **challenges and opportunities** for business applications

and space solutions: (i) a resilient and inclusive society, (ii) competitiveness in a sustainable digital economy, (iii) acting for a green and sustainable future, (iv) the advent of commercialisation in space.

She continued presenting various **solutions and initiatives** ESA is involved in:

- **EFFORS** (Enhanced Flood Forecasting System for Critical Infrastructure Protection in Medium Size Alpine Catchments), a 24/7 service of email/SMS warning with information update 1h piloted for the Austrian motorway operator ASFINAG, Regional Hydrological Service of Styria and Energie Steiermark. The SatCom ensures quasi real time data communication in critical situations (floods) and in remote areas; the SatEO ensures the improvement of land use and land cover information.
- **OWA SIS** (Observation of Water Availability – System of integrated services) by Hydrologic Systems BV, Hydrologic, Research BV, e-LEAF (NL), for a daily historic, current and forecast soil water storage capacity and to get a better water allocation and reduce flood and drought.
- At COP26, the signature of a **Memorandum of Intent** with CEO Water Mandate, on space technologies and applications for Net Positive Water Impact.
- **SES5G** (Secure Environment supervisor empowered by Satellite and 5G technology) to manage the wide urban and sub-urban green areas and contribute to a significant reduction of events such as fires, crimes and other administrative offenses), with satellite connectivity using 5G seamless networks, UAVs and Satellite Earth Observation (EO) for fuel maps (with the pilot test partner Law Enforcement and Emergency Response services along the Castel Fusano Pine Forest reserve (Rome, Italy).
- **B-SURE**: a rapid collection and bandwidth-efficient secure communication of operationally relevant field information including visual-situation awareness tools fusing high-resolution video and image contents with EO data/maps (used by German firefighters in 2021 flooding).
- **B-Life** (Biological Light Fieldable laboratory for Emergencies) that is a multimodal communication service platform (hub), with a rapidly transportable bio-laboratory bringing a biological diagnostic capability as close as possible to heart of a crisis area. The Satellite connectivity and GNSS services guarantee continuous monitoring in areas not covered by terrestrial connectivity.

Ms. Rinaldo continued with **Space Systems for Safety and Security (ESA 4S Programme)** introducing the values of 4S (secured, resilient and sovereign solutions for ensuring trust in the digital infrastructures), the secure communication users (connected vehicles, critical infrastructures, maritime search and rescue, impact zones, critical applications, in-field connectivity). In the frame of such Programme, PSCE and ESA have signed a Memorandum of Intent (MoI) to support the use of satellite applications for public safety, and PSCE collaborated on the good conduct of two user studies about “*Satellite Applications for Public Safety*”.

She presented a call for proposals whose planned issue is on Q1/2022: ***Space Applications supporting Digital transformation in Public Safety*** and the requirements to answer the call (more details at business.esa.int/).

Ms. Rinaldo concluded with the **ideal solution** for Emergency response: a unified, resilient, real-time and smart information network based on Observation (AI EO in space), Telecom

(5G/6G/Quantum/AI), Data Processing (IoT/AI), that sustains, secures, connects, protects and computes.

TOPIC 3: Mission Critical Applications using Broadband Communications: current and future solutions

1. *Towards an EU-wide interoperable communication system for security* - Max BRANDT, EC - DG HOME



Max Brandt, Policy Officer in DG HOME Counterterrorism since 2021 working on resilience. Before that, Max has worked two years in the unit dealing with innovation in DG HOME, following and promoting the Broadway project and developing it further towards the basis of an EU wide communication system for security. Before joining the Commission in 2019, he was working for 5 years in the European Parliament and 2 years at the German Police University.

Mr. Brandt started reminding the BroadWay EU-funded project's **ambition** and other initiatives that are more than projects on secure communications: they both fit with political and strategic EU context and are very concrete, in view of how end-users operate on the field. Their ambition is like tools such as Schengen information systems' one in the internal security domain: a new wide interoperable communications system is possible in Europe and deserves to be thought as well in the internal security domain, because it literally saves lives.

He mentioned how the European Union (UE) strongly encourages all the relevant stakeholders to be involved in the debate; it is not only related to internal security domain, but also to wider topics. At a political level, debates on Communication are shaping Europe: about the 5G, information security, data, strategic autonomy, resilience of Europe. And such resilience point brings together Communication as a technology and service, and also as a mean to ensure first response capability in case of disaster. This is why what is done in BroadWay or other initiatives in communications for public security and safety connects to important high level political debates: the ambition to **set up an EU wide interoperable communication system for security** is worth and promising.

Mr. Brandt then talked about the concern of the **existence of a clear mandate** to concretise such ambition. He confirmed that it is the case. On the first hand, in the very **global level**, EU citizens answered massively that they want an EU wide interoperable communication system; they ask EU to cooperate more in crisis management (78% in various polls). It is the same about fighting crime and terrorism. On the other hand, at the **political level**, such adherence is confirmed: (i) in June 7, 2021, the Justice and Home Affairs Council, in their final [Conclusions](#), underlined "*the importance of secure operational and EU interoperable communication [...]*"

and invites Member States (MS) to further support EU initiatives aiming at the improvement of existing systems and EU-wide interoperable communication systems for public safety, notably the Horizon 2020 BroadWay Project”; (ii) the Resolution of the European Parliament published on December 17, 2021 highlights “the importance of secure communications and secure communications infrastructure and [appoints] the Commission to plan the research and deployment of technologies to ensure the EU internal security”.

Mr. Brand continued stating that a very good **technology solution**, like successively BroadMap’s and BroadWay’s ones or smaller sector-oriented projects’ ones such as in mobile communications and secure apps for law enforcement, is necessary but **not enough**. On the first hand, the market situation, political considerations, national systems and legacies are in play. There is a need to **ensure coherence** and here is the role of EU level: try to structure, with MSs, various groups of stakeholders to stand together on elaborating such EU wide interoperable communication system. On the second hand, there is a need to **be more visible** and raise awareness on the topics and different related initiatives. That’s why the DG HOME communicated a lot in Brussels at the end of 2020, to the Commission and different innovation and public responders networks, about how EU agencies like eu-LISA, Frontex, etc. can play a crucial role in supporting what MS are doing in the domain.

He mentioned that **the Commission supported BroadWay** to approach the European Investment Bank (EIB) and gathered different stakeholders in the process, underlining the need to have the most forces possible on board if we want an EU wide solution, given the complexity and hugeness of the task.

Early 2022, DG HOME will mobilise a continuous funding path from its **Internal Security Fund (ISF) for BroadWay Project**, to support preparation towards BroadNet, which would realise operational mobility, the key outcome of BroadWay.

Mr. Brandt reminded that everyone who can **raise awareness** of BroadWay, or such projects should be self-confident as DG HOME is willing to integrate the most relevant expertise possible to reach its ambition. In the political level, in the ministries, outside the communication departments, there is a need to make it clear that it is very relevant to invest in. The very recent challenges Europe faced last summer (floods, wildfires, cross-border crimes), let him think that communicating more will have an immediate positive impact.

He tackled the critic of a too ambitious and complex system, including in terms of cooperation, that would be the EU’s wide one. Despite a lot of things ongoing that are a chance, there are also risks to the elaboration of a **community system**: the deployment of national broadband systems, technological progress in other parts of the world. He warned about the fact that having such opportunities now, if we don’t succeed in the coming years, we will have to wait the next 25 or 40 years for the next peak shift, because one MS will do in a way, others in another way, and again we will have a fragmentation.

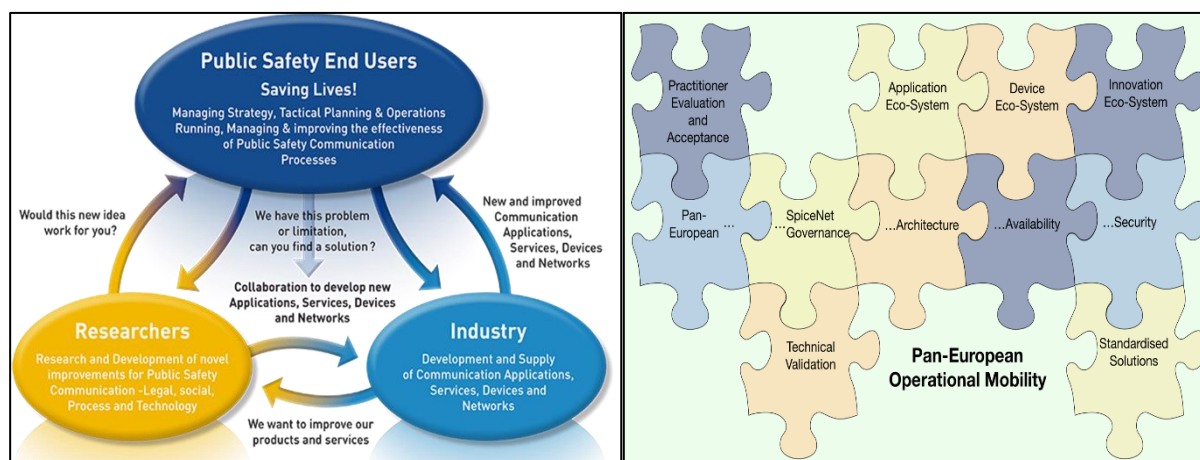
Mr. Brandt concluded highlighting all the **efforts** made by PSCE, BroadWay consortium, stakeholders from other related projects, MS and institutional colleagues that work on interoperable communications for public safety and shared his wish that all the efforts made will be reflected in policy processes. DG HOME is keen to take it forwards open to any support to carry the initiative out.

2. BroadWay: From Solutions prototypes to Pilots implementation - David LUND, PSCE



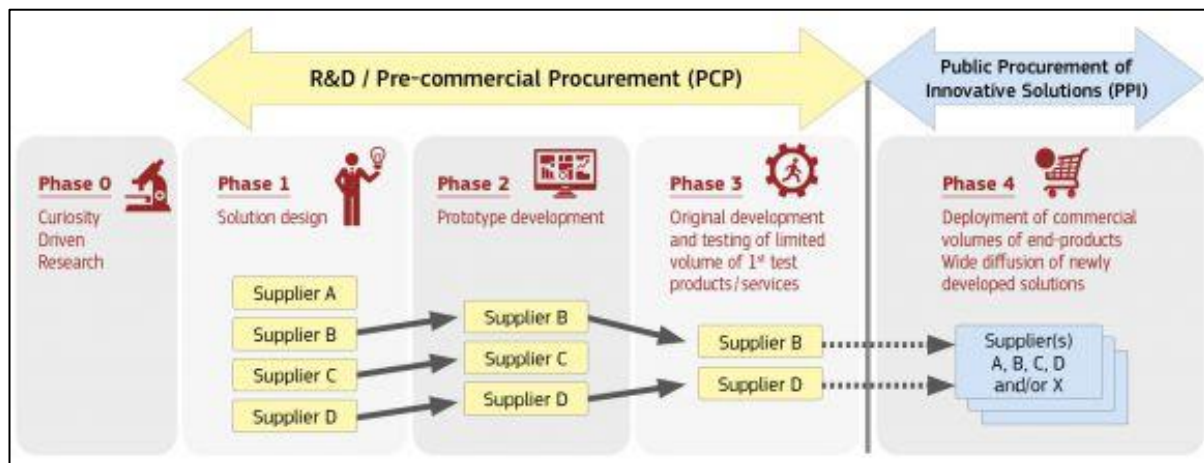
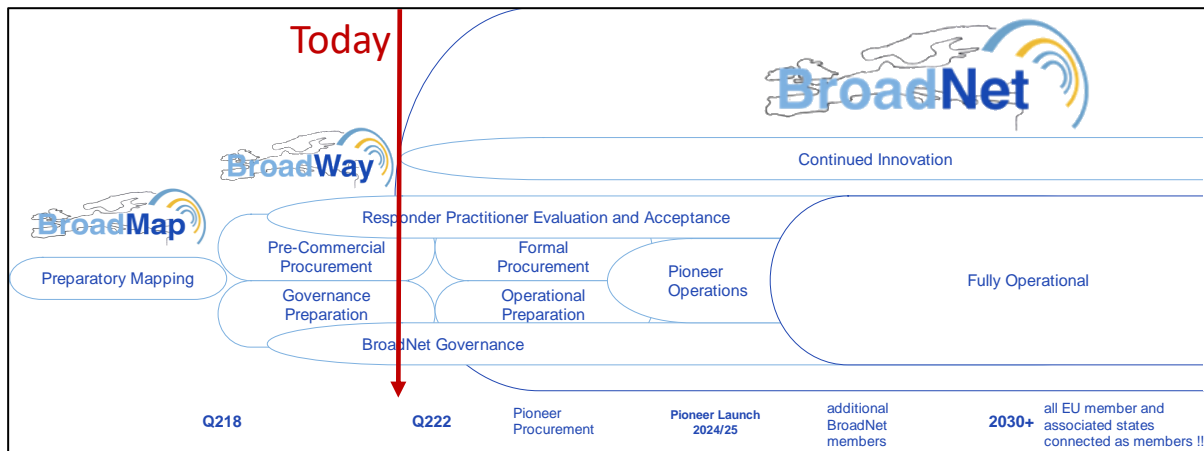
David Lund is board member of PSCE and coordinator of project BroadWay, BroadWay is a key activity that will jointly procure pre-commercial solutions to enable mobile broadband for public safety practitioners, providing them with operational mobility; allowing the ability to carry out their important lifesaving and crime fighting roles, whenever they are in Europe, and whenever they need to. David's experience in Public Safety Communications dates back to the late 1990's where involvement in research projects lead to the first demonstrations of medical telemetry and multimedia over the first implementations of circuit switched TETRA. David was an active contributor to the TETRA standards as ETSI special task force expert on many occasions covering aspects of coding, modulation, RF extension down to VHF and definition of the Multimedia Exchange layer (MEX).

Mr. Lund started reminding what is **PSCE** (figure here below), as Coordinator of BroadWay, the **aim** of such project that falls under topic SEC-04-DRS-2017 and call DRS-18-2015 (enable interoperable next generation of broadband radio communication system for public safety and security), the BroadWay **partnerships**, the **Practitioner Evaluation Team** led by the Bavarian Red Cross, and the **ambition** of BroadWay to be a pan-European Operational Mobility system (figure here below).



Mr. Lund then reviewed the past Design Phase and Prototype Phase with Airbus Defence and Space, Frequentis and Leonardo competing consortia, and the third **ongoing Solution Pilot Phase** that started on October 8, 2021, with Airbus Defence and Space, and Frequentis consortia.

Mr. Lund continued with the review of the transition from BroadWay to BroadNet, realising the **Operational Mobility** (see figures here below).



He continued with the **scope** of BroadWay solutions:

- Radio Access sharing commercial mobile (national level).
- Roaming - national and international
- Maintaining Service Quality, Priority, Pre-emption across multiple domains
- Seamless Continuity of service
- Standardized Mission Critical Services - MC-PTT, MC-Video, MC-Data
- Access to other information services – other PS Apps
- Harmonized Security – systems and services managed in different domains (responder networks, national networks, international networks)
- Eco-systems of Devices, Applications, and further Innovation

Mr. Lund concluded saying that BroadWay contributed to BroadNet preparation in terms of **governance** (for a live pan-European Operational Mobility) and **comprehensive technical view** (legal, financial, regulatory, policy, political ones), reminding that it's not all about technical: both responder practitioners and supply chain actors are involved in the process. Such work for BroadNet will be continued next year under the ISF funds.

3. National Broadband Applications

1. The Netherlands: Introduction and use of mobile applications within the Dutch PPDR organizations - Feiko VERMEULEN, Dutch National Police



Feiko Vermeulen has been the Service Manager of C2000 for over a decade. Within the Dutch Police, he works at the Department for National Control Rooms that provides control room services for the Fire Brigade, Ambulance, Military and Police forces. He is specialised in “cross-border communication and international cooperation” and was involved as a project manager in ISITEP EU-funded project, a three-country pilot between Belgium, Germany and the Netherlands. He is currently involved in the EU-funded project BroadWay.

Mr. Vermeulen started with the review of the **development and usage of (mobile) applications**. The **landscape** of PPDR organisations in the Netherlands is (i) 11 units and 1 organisation for Police and Military Police, and (ii) 25 regions and organisations for Fire and Ambulance services. The **key elements** for a successful application introduction by the Police are the (i) *Vision* on how to work in a mobile environment (2014), (ii) *Policy “mobile if possible”* (2014), (iii) *Application renewal* (2014), (iv) *Operational trials* (2014-2018); not forgetting the MEOS (More Effective On the Street) approach in police operations (2018).

He continued with the concern of **supporting interactions with the public**: (i) **police website** for privileged contact point, victim support, to check online seller and get updated on burglary situations in the neighbourhood, and (ii) the **equipment** of Dutch National Police officers and staff with 63 000 smartphones to complete (new) tasks more quickly (in the frame of MEOS).

Mr. Vermeulen then mentioned the mobile applications to officers and staff, supporting the operations: **Blue program** integrating a personalised homepage listing the big weekly incidents, the wanted people for arrest, the missing persons, other alerts and instruction videos; **Special Command and Control apps** for Police and Fire brigades – *DragonForce* as a workforce collaboration tool to share location and incident information, to provide enhanced situational awareness and collaboration and to improve operational outcomes including counter-terrorist situations, and *LiveOp* for operational use; **PTT-app and Dispatch app** for all the PPDR organisations, as a high-level SaaS (Software as a Service) commercial off-the-shelf with governmental security level (25 000 simultaneous users, 1000 active groups); **other mobile data and applications used by fire and ambulance services** respectively for location, address, floorplans, preparation plans of buildings and crash and recovering information on cars, and for sending patient vital functions to the hospital and access to patients medical dossiers.

Mr. Vermeulen concluded with some **challenges** for the use of mobile applications, in terms of experiments, training, technology improvement, lock-in of application or vendor, security hurdles to overcome, and with the review of the “*Anders werken*” Security Guidelines released since Covid-19 emerged.

2. Finland: How 5G, AI and Cloud can enable new public safety services - Kari Junttila, Erillisverket



Kari Junttila is Senior Research Specialist in Information Technology at Emergency Services College Finland, R&D Services. His responsibility areas are ICT technology of the operational systems for the emergency services and also coordination of R&D activities which improve usage of ICT technology in Finland. He has a broad working experience from cellular networks and technology management to financial aspects in TeliaSonera Finland, TS corporate level and international operations. He has also worked 16 years in the Finnish Air Force with radar systems.

Mr. Junttila started with a review of the **Mission Critical Ecosystem** as resources to public safety that is beyond the business and consumer services level: **mission critical communication system** (baseline that took advantage of the introduction of the broadband systems to enable new types of services such as video and broadband data), **data centres and secure cloud** (to store all the data in a confidential and secure way), **algorithms and data lakes** (both to process the collected data into valuable information and to store it in a sharable way between different organisations), **situation awareness services** (that uses AI to select the relevant information among the huge quantity of data to be presented to the public safety personnel).

He continued with the example of the **drones** in the public safety operations. At the moment they are mainly set up in a manual way, so an operator controls a drone keeping an eye on it, but there is a need to watch the live video-feed from the line of sight of the drone. Nevertheless, some **non-line-of-sight drones** are allowed in public safety and flying thanks to 5G technology: 5G, Cloud, AI enable more autonomous drone operations. With robotics, edge computing and AI, there will be no need of operators to fly the drone or analyse live its video-feed.

Mr. Junttila then mentioned the **Suomen Erillisverket's Strategy for AI** and the two main concerns that came up proceeding the interview of various organisations: (i) despite reducing manual tasks, there is a “*shortage of resources, not enough people specialising in data analytics*”; (ii) even if computers support decision-making in difficult or fast situations, “*utilising AI is not something that everyone can easily do, it requires additional resources*”. But AI actually ensures the process of turning unstructured and exhaustive data into precise and relevant information with the same personnel resources working better.

He mentioned then the **Augmented Reality (AR)**, considered from some people as science fiction (e.g., Google glasses failure), and took the example of the deal between the US army and Microsoft to produce 120 000 AR headsets (for 22 billion dollars): AR technology evolves

very fast, and the technology is truly usable and robust enough to be used in hostile environments.

Mr. Junttila concluded on the promising but nevertheless complex **future** of mission critical communications and services: public safety organisations are not able to run their own services, end-to-end solutions; they have to turn to the private sector that produces the technologies. There is a high need of public-private partnership, more than before, to spread the 5G access, secure cloud and AI to all public safety services.

3. France: Réseau Radio du Futur Programme - priority mobile, secure, high speed, resilient communication system - Renaud MELLIES, French MoI



Renaud has been working in the telecommunications industry for 20 years before joining the RRF program led by the French Ministry of Interior in 2020. RRF, the future French PPDR Broadband Network, will guarantee a smooth transition from legacy heterogeneous narrowband networks and will respond to the ever-growing operational needs expressed by French PPDR users. Renaud has been heading standardization and innovation efforts and was recently appointed as head of international cooperation.

Mr. Mellies started with the **replacement of legacy networks** in the frame of the “Réseau Radio du Futur” / “Radio Network of the Future” (RRF): from the voice-centric to multimedia applications. RRF is an innovative communication system giving access to the best current technologies and adapted to public safety operational needs on the field but also in control rooms.

RRF will replace the current narrowband networks because there are increasing needs for interoperability, data and video sharing, an ending of network system maintenance, and obsolete devices rejected by users; in other words, a technological gap between communication tools available for emergency and security services (1,5/2G radio devices) and 4G/5G smartphones used by citizens.

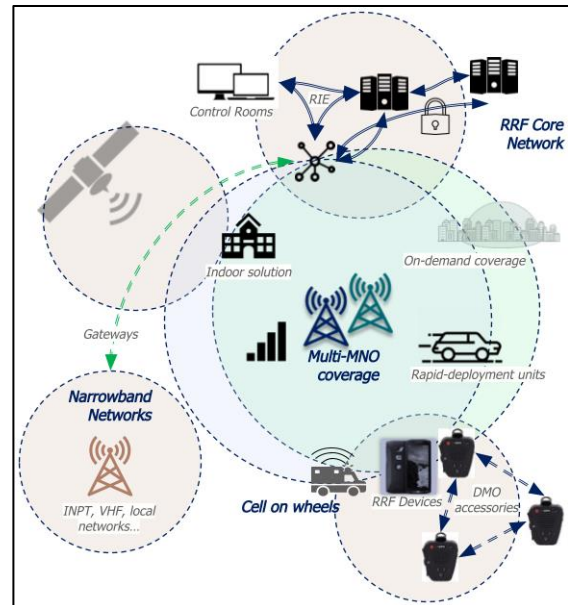
Some services and features will be set up for **operational communications**, in line with current communication standards: among other things, Mission Critical (MC) applications, 4G/5G reliable exchange data rate, prioritized access to the coverage of 2 Mobile Network Operators (MNO), encrypted and recorded communications with a secured transmission of all the data included medical data. RRF will provide multimedia apps on devices not only on field but also in **control rooms** with complete toolsets including Application Programming Interfaces (API) enabling smooth integration.

He continued on the **RRF Mission Critical Ecosystem** delivering high-quality, resilient and reliable MC services and applications relies:

1. Secured storage in a centralised datacentre, hosted in government-owned infrastructure; high-availability, fault tolerance and redundancy; standardised mission critical communications.

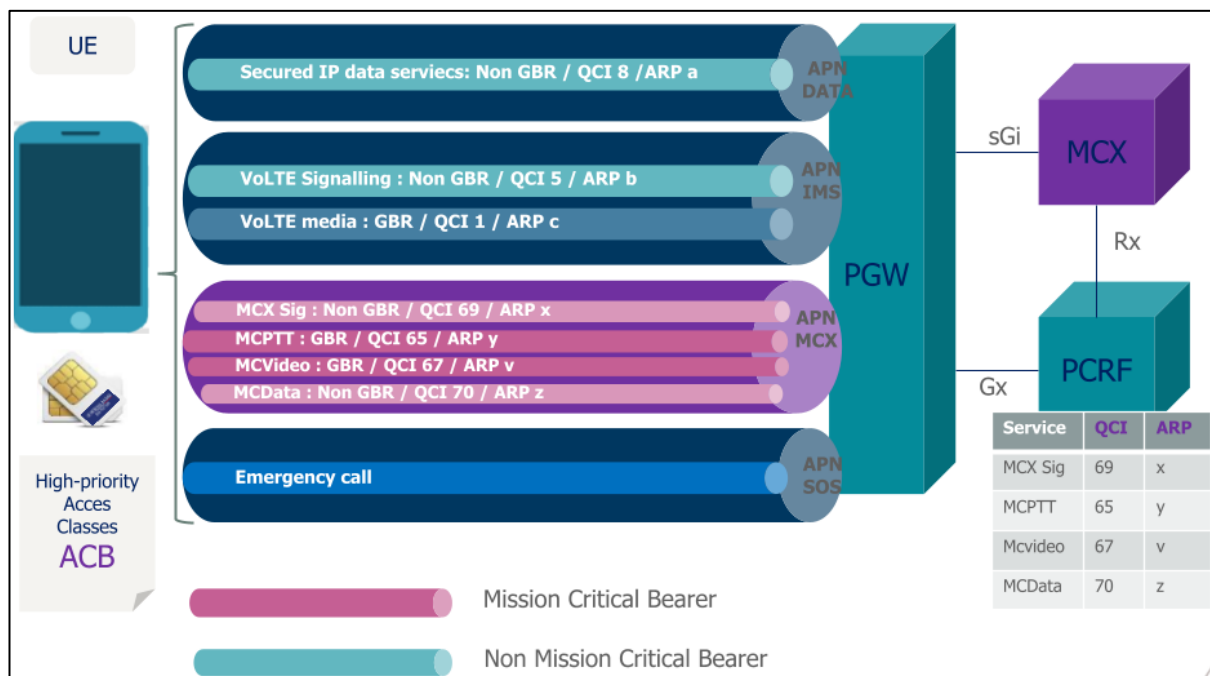
2. Nationwide coverage; gateways for legacy networks interoperability; international roaming; 5G non-terrestrial networks study.

3. Ad-hoc coverage: cells on wheels; direct mode for off network communication; on-demand coverage for anticipated events; rapid response vehicles for emergency purpose.



Moreover, devices (such as handsets, tablets, and other certified devices) are carefully selected to fulfil all types of **requirements**: the ones induced by the Request for Tender's selection criteria, including on hardware and firmware, operation system, application client ecosystem; access to MC services using only RRF Sim card; MCX services, security and operational requirements.

Also, MC applications are making use of MC services and carefully chosen MC quality of service, priority and pre-emption: QCI, ARP, ACB.



Mr. Mellies then broached the topic of **Mission Critical, Business Critical and Public applications**, that are key for public safety, and the fact that multiple applications may coexist on a MC device: (i) MCX applications making use of MCX services (MCPTT, MCData, MCVideo) that require mission critical QoS, priority and pre-emption; (ii) lower priority applications such

as business ones (developed internally by PPDR organisations or third-party business applications) or public ones (from a restricted list, carefully curated given the specific needs and security constraints). Not forgetting that MC applications shall not be impacted by lower priority applications: priorities, permissions, dependencies shall be thoroughly assessed.

He concluded on the **device and application management** concern that is critical; the RRF has established certification and validation processes. On the first hand, the Enterprise Mobility Management (EMM) that comprises the Mobile Device Management, Mobile Content Management, Mobile Application Management. On the other hand, the certification and validation processes from technical pre-requisites (software and hardware compatibility) to different kinds of validation.

4. Belgium: Towards Mission Critical data in Belgium - Lessons from the past - Visions for the future – Jo DEWAELE, ASTRID

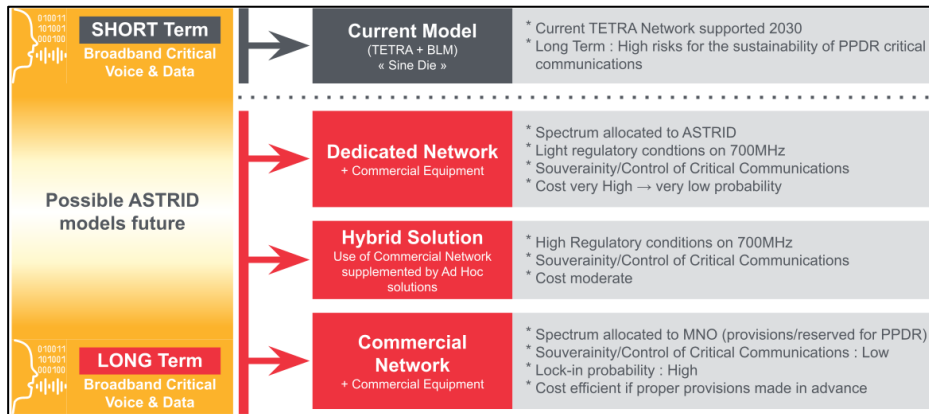


Jo Dewaele has been involved in ASTRID for more than 27 years. In 1994 he became involved in defining the user requirements for the ASTRID project as a representative for the Judicial Police and the Ministry of Justice. In 1998 when the ASTRID company was created he became responsible for the radio network rollout in the pilot province. Since then, he has served ASTRID in various positions: ETSI and 3GPP standardisation, customer technical advisor, product development, project portfolio management, enterprise architecture. In March 2021, he took a new role in ASTRID as Marketing Strategy Team Leader.

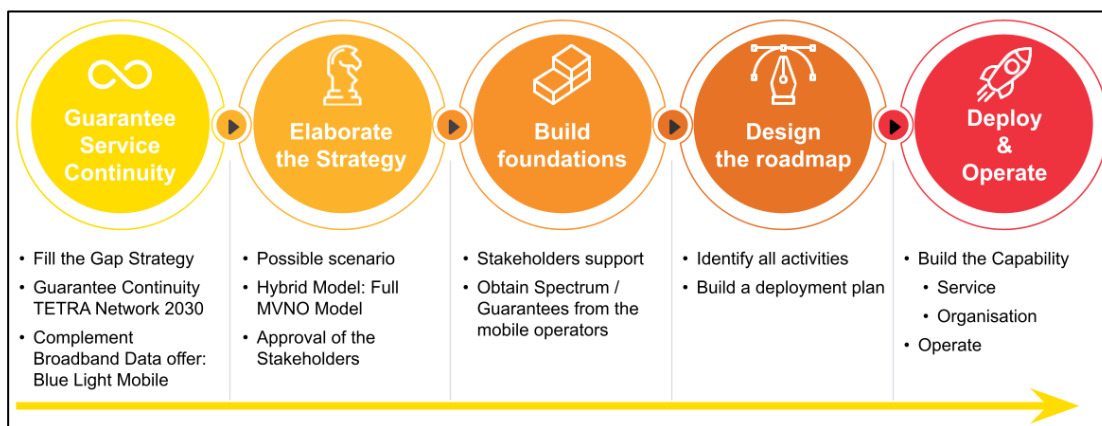
Mr. Dewaele started considering the **need for a Mission Critical Network**, taking the example of the flooding in Belgium that happened in July 2021. After recapping the geography of Belgium, phases of the alert in link with the water levels, aftermath of the disaster, and rescue material used, including the communications tools that were DRP radio and BCM call taking, he reviewed comparatively all the critical dimensions that are covered by Business Critical (BC) and Mission Critical (MC)

DIMENSION	BUSINESS CRITICAL (BC)	MISSION CRITICAL (MC)
Guaranteed Communications	In reasonable or normal "critical" conditions	BC conditions + "operational" and "technical" crisis
Impact when failure	Inconvenient for the user, with no particular major impact	Risk of endangered lives and significant material damage
Concept Principles	Profitability, competitiveness and sufficient reliability in most situations	Full redundancy, high hardening, maximum reliability, priority and preemption
Coverage	≤ 99,5%	> 99,9%
Back-up during power outage. (High risk for BE!)	≤ 2 hours (LTE less then 2G!)	≥ 8 hours
Evolution of applications and functionalities	Developments follow, even lead to the rythm of the market	Need for standardization before reaching MC level
Targeted Public	Business organizations, private users, leisure, etc.	Public security actors and associated organizations
Type Network	Commercial networks	Hardened network

He continued presenting the **ASTRID Strategy** to next generation of MC Communications:



Also, the **steps** until their deployments:



Mr. Dewaele **compared** then the Mission Critical Broadband (MC BB) and Narrow Band (NB) TETRA in terms of status and event information, geolocation, database queries, pictures and video quality; the MC data application needs have not changed while the amount and quality of information have changed.

He mentioned the **Narrow Band TETRA (2G)** experience (faster progression of WP 3G mass market, NB dedicated niche ecosystem, failure of MC data on NB TETRA) and the **lessons for the future BB 4G/5G MC apps** (to evolve at the speed of mass market, to be compatible with the mass market ecosystem, MC operators offering has to be comparable with the mass market operators offering, to offer an extra layer of security).

Mr. Dewaele concluded about the **interoperability** as essential for Mission Critical Voice and Data communications, stating that (i) the MC BB aim should not make us forget the basic interoperability need fulfilled with NB TETRA – a nationwide common communication system for all the public safety services, and (ii) the MC BB should reach the international interoperability need that NB TETRA was unable to reach – an international interoperable communication system for all public safety services in the EU.

4. EPICENTRE: 5G Experimentation Infrastructure hosting Cloud-native Netapps for PPDR - Ioannis MARKOPOULOS, NOVA



Dr Ioannis Markopoulos is leading NOVA's Innovation Department. He is a member of the Technical Chamber of Greece. Since 2007, he has been PMP certified. He has been working and leading numerous European and Domestic R&D projects in the domain of broadband telecommunications, value added services, management, etc. Moreover, he has participated in the Federation of Hellenic ICT Enterprises, promoting frameworks capitalising on EU structural funds. He actively participates in 5G-PPP TMV WGs and led the task force for the mapping of the vertical KPIs of ICT-19 and ICT-20 projects to the 5G network KPIs.

Mr. Markopoulos started with **5G-EPICENTRE** contribution to emerging PPDR needs, as an open and federated 5G end-to-end experimentation platform specifically tailored to the needs of PPDR software solutions.

He followed up with the 5G-EPICENTRE **factsheet** (ICT-41-2020 - 5G PPP – 5G innovations for verticals with third party services topic, from 01/01/21 to 31/12/23), **provisions** (lower entry barrier to PPDR market for SMEs and developers, accommodate an open access to 5G networks' resources (open-source repository for PPDR 5G NetApps), provide sufficient resources to cover the 3 ITU-defined service types (eMBB, mMTC, URLLC)), **highlights** (federate 5G platforms into an advanced, user-friendly, zero-touch orchestration single point of control, implement a repository of network functions (V/CNFs) and NetApps, participate to the cloud-native transformation of facilities and network functions), **objectives** (build an end-to-end 5G experimentation platform, pilot 5G systems in PPDR-based trials, cultivate a "5G Experiments as a Service" model, facilitate automation, continuous deployment and Multi-access Edge Computing (MEC), leverage AI for achieving cognitive experiment coordination and lifecycle management, implement impact-driven dissemination, standardisation and exploitation).

Mr. Markopoulos continued with the **5G-EPICENTRE infrastructure**: it brings together 5G-EPICENTRE brings together 4 geographically dispersed, end-to-end private 5G platforms, which support key 5G KPIs and allow cross-site orchestration and experimentation for PPDR solution vendors to validate NetApps reliant upon those KPIs (in Malaga, Aveiro, Barcelona and Berlin).

He shared with us the planned **cloud-native transformation**: (i) decoupling of network functions from virtual machines (VMs) toward Containerized Network Functions (CNFs), (ii) use of Container virtualisation technologies (Docker) and orchestration tools (Kubernetes – K8s), ideal for implementing the proposed architectures for emerging 5G networks and addressing their requirements.

Then he mentioned all the 5G-EPICENTRE **use cases**: Multimedia MC Communication and Collaboration Platform; Multi-agency, multi-deployment MC communications and dynamic

service scaling; Ultra-reliable drone navigation and remote control; IoT for improving first responders' situational awareness and safety; Wearable, mobile, point-of-view, wireless video service delivery; Fast situational awareness and near real-time disaster mapping; AR and AI wearable electronics for PPDR; AR-assisted emergency surgical care.

He presented the 5G-EPICENTRE **platform testing**: (i) Deployment and execution of the experimentation on top of the 5G-EPICENTRE infrastructure, (ii) Experiments designed to accommodate first responders' needs and requirements, and ensure fast service-level KPIs, (iii) Timetable (02/2022-12/2023).

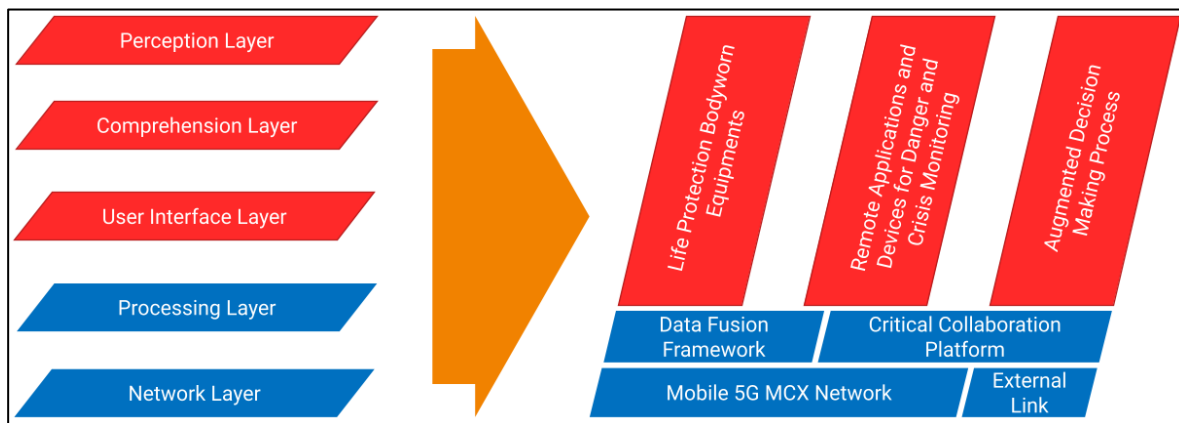
Mr. Markopoulos concluded with the presentation of the **5G-EPICENTRE Innovation Hackathon**: (i) Goals (bring together NFS/SDN and 5G research teams to make them design and deploy innovative mission-critical applications for first responders on top of the 5G-EPICENTRE infrastructure), (ii) Expected results (extend the capabilities of the 5G-EPICENTRE facility (capacities and repositories of NVF/NetApp solutions), and pitch, design, implement and demonstrate innovative PPDR solutions by third parties, (iii) Planning (workshops to get familiar with the 5G-EPICENTRE platform, draft of hackathon Open Call documentation, set up of hackathon web portal).

5. 5G critical applications development for First Responders - Drazen RIBAR, AIRBUS



Drazen RIBAR is a Research and Technology Project Manager at AIRBUS DS SLC. He started more than twenty years ago in the design and specification of embedded computers and integration of software for tools and network management. He moved to a new AIRBUS challenge for the built of a new portfolio around mobile Internet applications, Connected Devices and Smart Cities for Public Safety. After several years of sharing and collaborating with Public Safety users in order to address the use in the field of new technologies, he has been appointed Project Manager in Research and Technology team and he is involved in building and contributing to multiple collaborative European projects.

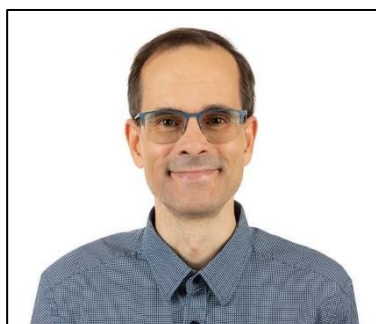
Mr. Ribar started with the presentation of **RESPOND-A project**: from *DRS02 – Technologies for First Responders* call and coordinated by the European University of Cyprus, it involves 34 partners and areas of expertise (among which 10 First Responders (FR) organisations), **to maximise Situational Awareness by introducing a joint Technological and Conceptual Framework** (here below the Five-Tier Architectural Structure for an Innovative Information Management System).



He continued with the presentation of **technologies and services** developed in the frame of the project: **(i) Life Protection Body worn Equipment** (to leverage FR safety knowledge, bring *easy-to-wear* Smart Wearable, ensure resiliency of data collection, participating to operational process and data collection standardisations, respecting the GDPR regulations); **(ii) Remote Applications and Devices for Danger and Crisis Monitoring** (to enhance crisis environment construction, take advantage of the easiness of deploying drones and robots, develop remote and distributed operations, support missions in dangerous environment); **(iii) 5G Mission Critical Services on the Field** (to develop and use 5G mobile and tactical infrastructures, 3GPP MCX on the edge services, satellite link for remote connection to C&C); **(iv) Augmented Situational Awareness for Decision Making** (to involve common operational picture, shared decision making process, AR for Mobile C&C, triage, smart data aggregation).

Mr. Ribar mentioned the **3 pilots based on real-life scenarios** of RESPOND-A (Search and Rescue in Spain, Earthquakes in Greece, Forest Fires in Cyprus), before concluding with the importance of the availability, reliability and efficiency, key concepts for **leveraging situational awareness on the field**.

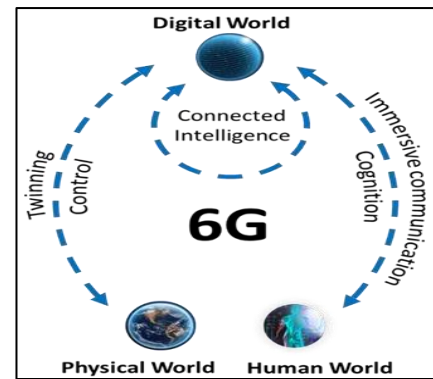
6. European Vision for the 6G Network Ecosystem: the voice of the European industry for the development, deployment and evolution of 5G - Mikko UUSITALO, Nokia Bells Lab Finland



Mikko Uusitalo is Head of Research Department Wireless Advanced Technologies at Nokia Bell Labs Finland. He is leading the European 6G Flagship project Hexa-X. He obtained a M.Sc. (Eng.) and Dr.Tech. in 1993 and 1997 and a B.Sc. (Economics) in 2003, all from predecessors of Aalto University. He has been at Nokia since 2000 with various roles, including Principal Researcher and Head of International Cooperation at Nokia Research. He is a founding member of the CELTIC EUREKA and WWRF, the latter one he chaired for 2004-2006. Mikko Uusitalo also is a WWRF Fellow.

Mr. Uusitalo started mentioning the **societal, EU policy and business drivers for 6G** development: address the United Nations' Sustainable Development Goals, having technology sovereignty, improve the economies of EU Member States, for instance.

He listed then the **main goals of 6G**, linked to connected intelligence, programmability, determinism, sensing, sustainability, trustworthiness, affordability and scalability, before going more into details for the **connected intelligence** goal that has a fundamental impact on the mobile network: immersive communication, cognition and twinning imply virtual representations in the digital world that have dynamic relations with sensors, screens and cameras; the connections between virtual representations in the digital world replace connections between mobile end-devices.



He continued with the **comparison of 5G and 6G KPIs**, in terms of capacity, user experience data rate, latency, device intensity, location accuracy and energy efficiency, mentioning the objective of the 6G as 10 times more performant than 5G, up to 30 times for location accuracy and 300 times for time efficiency. Not forgetting the KPIs of density, coverage, privacy and cost.

Mr. Uusitalo also presented the envisaged **key technologies for 6G** that have a strong impact on different 6G requirements and KPIs; considering that AI/ML mechanisms for the optimisation of the physical and higher layers will be an essential tool, and not forgetting the exploitation of properties from quantum mechanics promises unprecedented performance in quantum sensing, communication, security and computing:

- 1. Network Architecture and Control** – for efficient, sustainable, smart and trustworthy distributed computation, with the need of AI/ML, automatic resource control, and automatic distributed mechanisms.
- 2. Edge and Ubiquitous Computing** – driven by IoT, Industry 4.0, Smart Cities, to reduce delays, increase responsiveness and reduce data flows.
- 3. Radio Technology and Signal Processing** – because 6G networks will deal with more challenging applications requiring Tbps data throughput, sub-ms latency to the network layer, very low packet error rate, increased device density, ultra-low energy consumption, very high security, cm-level accuracy localization, etc. (with some key enabling technologies such as mmWave, THz and Optical wireless communication, (ultra-)massive MIMO, etc.).
- 4. Optical Networks** – to develop a smart optical transport connectivity always available, intrinsically secure, green and with flexible scaling, exploit all dimensions in space and frequency and then open new optical wavelength bands and space division multiplexing.
- 5. Network and Service Security** – as cybersecurity must evolve as the system does and because the highly distributed computing and connectivity architecture of 6G create an attack surface wider and more complex than 5G, new approaches for security must be developed.
- 6. Non-Terrestrial Communication** – architecturally designed as a single access network with a constellation-hierarchy, with computing and storage in the sky, it comprises resource optimisation, dynamic spectrum management, coexistence and sharing, flexible and adaptable radio access technologies, software-defined payloads, and new antenna designs and components at THz.

7. Devices and Components – to address radio frequency and optimal challenges such as, respectively, phase noise, MIMO/hybrid Beam Forming for large arrays, transceiver architectures, etc., and monolithic integration, CMOS processing, photonic devices, etc.

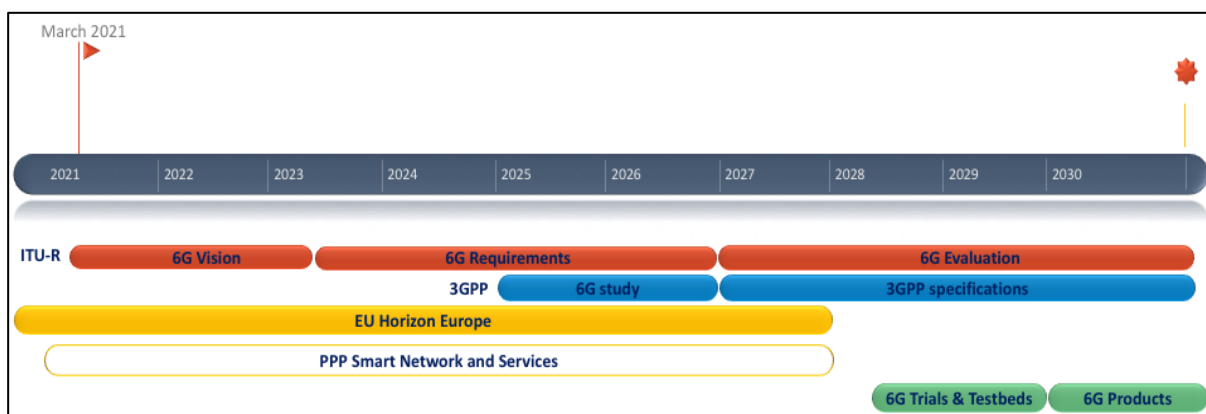
Mr. Uusitalo followed up with the **6G infrastructure as a Smart Service Execution Platform** (in comparison with 5G): (i) an infrastructure that ensures a flexible on-demand provision, is capable of resource control and comprises full-service platforms; (ii) a mobile system architecture that brings novel service requirements, expected novel capabilities and the push of the programmable elastic system, so the mobile system looks like a computer program executed within the programmable infrastructure.

He analysed then the 6G architecture to underline few **principles for a future mobile communication system**: (i) flexibility and functionality are essential and should not add to the overall complexity; (ii) “AI everywhere” should lead to the improvement of the network performance and the delivery of AI-as-a-Service in a federated network; (iii) trustworthiness is central.

Mr. Uusitalo concluded by stating that **6G will play a key role for societies** of the future and should be supported by global standards and renewed regulations, and that AI/ML mechanisms will be crucial and reusing universal infrastructure is required to provide more diversified services and achieve the increased sustainability awareness.

Jointly to the envisaged **timeline** for 6G development (here below), he gave some **recommendations** as it follows: **(i)** new regulations and ethics principles are needed to address certification and litigation; **(ii)** additional spectrum is needed for NTN systems and other actors; **(iii)** EU regulation will be needed to help new players to emerge and make sure that sovereignty and security requirements are addressed; **(iv)** the production and consuming of services, materials or energy should be done with moderation; **(v)** new professional skills will need to be developed.

*“To compete with future’s 6G enabled products in defence, automotive, white goods, industrial machinery, consumer goods, etc, Europe needs a **world-class competence resource pool** in wireless and wireline communications, microelectronics (at least in design), photonics, and software in industry as well as in academia, strengthen by a **proactive Regulation adaptation** to create strategic and business opportunities for EU companies.”*



Funding Opportunities

1. Internal Security Fund (ISF) - Arnoud HEERES, EC - DG HOME



Mr. Heeres is a Programme Manager at the European Commission (DG HOME), since 2015, focusing on law enforcement cooperation and digital security policies, including: ISF (Police) portfolio; the EU projects on Cybercrime, Drugs, Forensics, Schengen, Police Cooperation; specific police networks such as ENFSI, AQUAPOL, TISPOL, EuNAT, ECTEG, MAOC, ENFAST, EPRIS, ENLETS, UMF, WPGA, EACTDA; coordination with DG JUST, INTPA, NEAR for Security; coordination with agencies like Europol, CEPOL, eu-LISA, EMCDDA.

Mr. Heeres started presenting the **Directorate E – Migration and Security Funds, Financial Resources** and its **Unit E4 – Union Actions and Procurement** as well as the scope of the DG HOME Funds **AMIF** and **ISF** that complement EU countries' efforts and strive to provide additional value (in the management of migration flows and asylum requests, EU external borders, crisis and crime prevention).

He presented then the **ISF Implementation modes** ((2014-2020) Union Actions and Emergency Assistance management by the EU Commission (EC), National Programmes managed by EU countries), **ISF-P Specific Objectives-Allocations** (Technical assistance-police: 36 million euros, Risks and crisis: 155 million euros, Preventing and combating crime: 561 million euros), **ISF Regulation for the Multiannual Financial Framework (MFF) 2021-2027, DG HOME Funds 2021-2027** (19,3 billion euros for AMIF, BMVI, ISF), **EU budget per domain**, showing political priorities, **ISF total budget 2021-2027** (1,9 billion euros), **Home Agencies** and related budget (EASO, FRONTEX, eu-LISA, EUROPOL, CEPOL, EMCDDA, respectively 1,2, 6,4, 1,7, 1,3, 0,08, 0,1 billion euros).

Mr. Heeres also presented the **ISF's management modes** (80% shared, 20% direct), **beneficiaries** (State/Federal Police, Customs and other specialised law enforcement services, local public bodies, NGOs, IOs, Union agencies, private and public law companies, networks, Research institutes and universities), **policy objective** (contribute to ensuring a high level of security in the Union, in particular by tackling terrorism and radicalisation, serious and organised crime and cybercrime as well as by assisting and protecting victims of crime), **specific objectives and related resources allocation** (increase the exchange of information, intensify cross-border joint operations, strengthen capabilities to combat and prevent crime and terrorism).

He gave an overview of the **European Multidisciplinary Platform Against Criminal Threats (EMPACT)** that is a security initiative driven by EU Member States to identify, prioritise and address threats posed by organised and serious international crime. In 2021, EMPACT became a permanent instrument, as set in the Council conclusions on the permanent continuation of the EU Policy Cycle for organised and serious international crime. Its priorities for the next

cycle are the high-risk criminal networks, cyberattacks, trafficking in human beings, child sexual exploitation, migrant smuggling, drug trafficking, fraud, economic and financial crimes, organised property crime, environmental crime, firearms trafficking.

Mr Heeres mentioned the scheduled **ISF Calls for proposals (2021-2022)**: **a)** to support small companies in implementing the regulation to address the dissemination of terrorist content online, **b)** for actions supporting the implementation of the EU Counter-Terrorism Agenda (including public spaces, CBRN-E, unmanned aircraft system), **c)** on Cybercrime and Digital investigations, **d)** on the prevention of child sexual abuse, assistance to victims of child sexual abuse and tools to detect child sexual abuse online, **e)** data sets for the European Data Space for innovation, **f)** on Common Operational Partnerships to prevent and fight against migrant smuggling with competent authorities of third countries, **g)** on actions against trafficking in human beings, **h)** on better law enforcement in the area of illicit drug trafficking and on support to demand-focused initiatives in the fields of drug policy, **i)** on the fight against corruption.

Also, the **ISF Funded Networks (2021-2022)**: EU High Risk Security Network, European Network of Fugitive Active Search Teams (ENFAST), European Explosive Ordnance Disposal Network (EEODN), European Anti-Cybercrime Technology Development Association (EACTDA), European Police Records Information System (EPRIS), AQUAPOL Network, EU Air Marshals Network, European Cybercrime Training and Education Group (ECTEG).

He underlined the **Article 5** that limits the scope of IFS support: are not eligible the (i) actions with a military or defence purpose, (ii) equipment of which the primary purpose is custom control, (iii) coercive equipment including weapons, ammunition, explosive and riot batons, except for training purposes.

He reminded the **ISF novelties**: a) increased flexibility, b) actions eligible for higher co-financing, c) possibility to use operating support, d) simplification with a common rule book; and the synergies with other funds: European Social Fund+, European Regional Development Fund, Horizon Europe, Digital Europe, Custom control equipment, EU Civil protection mechanism, SRSP, Neighbourhood, Development and International Cooperation Instrument (NDICI), Instrument for Pre-Accession Assistance (IPA).

Mr. Heeres concluded with the **ISF implementation timeline** and the approval of Member States programmes by the first quarter of 2022.

2. SNS (Smart Networks and Services): the voice of the European industry for the development, deployment and evolution of 6G Smart Networks and Services - David LUND, PSCE



David Lund is board member of PSCE and coordinator of project BroadWay, BroadWay is a key activity that will jointly procure pre-commercial solutions to enable mobile broadband for public safety practitioners, providing them with operational mobility; allowing the ability to carry out their important lifesaving and crime fighting roles, whenever they are in Europe, and whenever they need to. David's experience in Public Safety Communications dates back to the late 1990's where involvement in research projects lead to the first demonstrations of medical telemetry and multimedia over the first implementations of circuit switched TETRA. David was an active contributor to the TETRA standards as ETSI special task force expert on many occasions covering aspects of coding, modulation, RF extension down to VHF and definition of the Multimedia Exchange layer (MEX).

Mr. Lund introduced his presentation with the **NetWorld 2020 Strategic Research and Innovation Agenda 2021-2027 "Smart Networks in the context of NGI"**, that is the foundation for the definition of the R&I technical thematic of the SNS work plan and work programme.

He presented the proposed structure of the NetWorld 2020's Work Programme: **(i) 5G Evolution with Stream A (RIA) – Smart communication components, systems and networks for 5G mid-term evolution systems** (it follows an evolutionary path towards the development of 6G networks and the proposed research topics are selected in such a way to create a complete system view when these are considered all together) and **Stream D (RIA) – Large scale SNS trials and pilots with verticals** (large Scale SNS Trials and Pilots. Explore and demonstrate technologies and advanced applications (e.g., Immersive communication, holographic telepresence & Augmented Reality / Virtual Reality (AR/VR), etc.) as well as advanced services in the vertical domains (e.g., connected mobility and smart transport and logistics, media and entertainment, public safety, e-Health, smart factories, smart cities etc.)); **(ii) 6G with Stream B (RIA) – Research for radical technology advancement towards 6G** (revolutionary research for radical technology advancement towards 6G. Low TRL technologies that are expected to deliver in real life networks in a mid and/or long-term time period) and **Stream C (IA) SNS experimental infrastructures** (SNS experimental infrastructures to be used during the second phase of the SNS by other Streams).

After showing the **SNS Roadmap and interlinking of the Streams in different phases**, Mr. Lund concluded going more into details for each Stream:

- **Stream A – 5G Evolution:** (i) Radio (address basic building blocks and develop RAN systems), (ii) Architecture and core (evolved architectures, advanced cloud and edge solutions, converged packet-optical transport network), (iii) System and security (secure and reliable "softwarisation", real-time zero-touch service technologies).
- **Stream B – Research Foundations for 6G:** to provide the research foundations for low TRL technology advancement in preparation for the upcoming 6G networks.

- **Stream C – Experimental Infrastructures:** (i) provide pre-6G experimental infrastructures, (ii) focus on the integration of new components/technologies, (iii) use the outcome for further validation, (iv) Streams A and B expected to deliver proof of concepts.
- **Stream D – Large Scale Trials and Pilots with Verticals:** (i) demonstrate technological and business validation with verticals, (ii) foster a close cooperation between ICT and other application domains stakeholders, (iii) leverage existing platforms project such as 5G Infrastructure PPP, End-to-End Facility, Vertical Pilots, IoT and Cloud platforms and projects, (iv) explore and demonstrate technologies, end-devices, communication components applications, (v) demonstrate Europe's leading solutions, (vi) involve SMEs, scaleups and start-ups.

PANEL DISCUSSIONS

Around 2 hours of panel discussions were spent during the conference, giving the chance to every speaker, even remotely, to answer questions from the audience and create depth. It was a great opportunity to share about EU institutional concrete initiatives incoming, to debate some topics in a more technical way, and offer participants practical information of funding opportunities that are a way to participate in shaping the future of Europe.



Exhibition Areas

In the two days of the conference, 10 exhibitor organisations held a booth; the occasion for all the participants to discover more in details all the solutions and services provided by the different exhibitors that could, in return, network and promote their activities in a warm and personalised way.



PSCE General Assembly & Committees

Despite numerous PSCE Members were not able to join us in Brussels, PSCE successfully organised both its yearly General Assembly (GA) and a Committees Meeting. Besides the common administrative matters the GA involves, PSCE Members took the occasion to meet up again (or for the first time talking about some new Members that travelled to Belgium), share views on the addressed topics, and agree on holding strategic positions as members of a forum.

Social event



At the end of the first day of conference, PSCE invited participants to a *brasserie* to have dinner together. The social event gathered the participants in the centre of Brussels; the occasion to share good food and conversations and take up physical social interactions again.

Not a member yet?

Join PSCE now as institutional member and take advantage of a range of benefits!

By **joining PSCE**, you automatically become part of the strong knowledge-sharing network bringing together users, industry and researchers in the field of public safety communications and information management systems. The diversity within PSCE's membership allows you to maintain regular contacts with your counterparts and other stakeholders in order to share and benchmark your experience.

By **becoming an institutional member**, your organisation will also benefit from a wide range of other benefits including:

- Access to enhanced and targeted **information** (Flash News, White Papers, Surveys, Conference documents).
- Facilitated **contact with EU institutions** to raise awareness about the community needs and topics and provide your contribution through your expertise.
- **Access EU Funded projects** (information on funding and partnership opportunities).
- Participate to the **functioning of PSCE** through vote and creation/participation to working group your experience.

Interested? Visit www.psc-europe.eu for more information or contact us at secretariat@psc-europe.eu.

Organised by

In collaboration with

Sponsored by