EU INNOVATION HUB

SHAPING RESPONSIBLE SOLUTIONS FOR INTERNAL SECURITY

EU INNOVATION HUB FOR INTERNAL SECURITY ANNUAL EVENT

in cooperation with the CERIS community

Brussels, 13-14 September 2022

The EU Innovation Hub is a cross-sectorial EU platform and aims to ensure coordination and collaboration between all innovation actors of the wider field of the internal security. The Innovation Hub, being composed of various EU Justice and Home Affairs Agencies, European Commission (including JRC), the Council General Secretariat and the EU Counter Terrorism Coordinator, works to provide the latest innovation updates and effective solutions to support the efforts of internal security actors in the EU and its Member States, including justice, border security, immigration, asylum and law enforcement practitioners.

For more information on the Hub, please visit this **link**

The EU Innovation Hub for Internal Security Annual Event Report
Shaping Responsible Solutions for Internal Security

Cite this publication: EU Innovation Hub for Internal Security (2022), The EU Innovation Hub for Internal Security Annual Event Report: Shaping Responsible Solutions for Internal Security

EU INNOVATION HUB FOR INTERNAL SECURITY

SETTING THE SCENE

Nicolas Bessot (European Commission DG Home) and Thierry Hartmann (French Ministry of Interior), co-chairs of the Steering Group for the EU Innovation Hub for Internal Security, welcomed the audience and set the scene for the event: joining internal security practitioners from the EU Member States and EU policy makers to discuss cutting-edge innovation topics.

Mr Luis de Eusebio Ramos, Europol Deputy Executive Director Capabilities, reflected on the Hub's progress since its inception in 2019 while also highlighting that continued efforts were needed in order to fulfil the ambitions expressed by the Hub's stakeholders. He highlighted the relevance of the Hub's pilot projects, in particular the Accountability Principles for Artificial Intelligence (AP4AI). He concluded by encouraging all Hub members to maintain or even increase their engagement in the Hub, in order to deliver meaningful benefits for the EU's internal security.

Panel 1
FUNDAMENTAL RIGHTS COMPLIANT USE OF DATA

Opening note: Michael O'Flaherty, *FRA Director*
Panellists: Ernesto La Mattina, *AIDA;* Thierry Hartmann, *French Ministry of Interior, co-chair EU Innovation Hub Steering Group;* Donatella Casaburo, *Project ALIGNER;* Emilie Né, *Project UNCOVER*
Moderator: Dr Teresa Quintel, *Maastricht University*

> ***"Fundamental rights should be brought into the process of developing innovative products for internal security from the beginning.***

The Director of the EU Agency for Fundamental Rights challenged the assumption that security and fundamental rights were in competition with each other. On the contrary, fundamental rights compliant security strategies are better strategies that make us more secure. He urged the audience to not only respect privacy, but also reminded of the potential chilling effects for all the other fundamental rights, including, for example, non-discrimination, the freedoms of expression, assembly and movement. Legality, necessity and proportionality need to be respected for any limitation on fundamental rights to be justified. Fundamental rights compliance had to be assessed at different stages: in the design, in the training, in the operation of the technologies, and following their application, and be embedded with oversight authorities to ensure a full respect for fundamental rights.
The panellists discussed how to prepare fundamental rights guidelines and assessments to mitigate risks and opacity in technology, specifically AI tools used by law enforcement. While the discussants recognized the importance of regulating AI, they agreed that innovation should not be hampered by over-regulation.

There was a plea for looking at the concrete use cases when training algorithms and applying AI solutions in practice, developing tools in a transparent way with respect for fundamental rights ensured throughout the life cycle. The panel concluded that fundamental rights should be brought into the process of developing innovative products for internal security from the beginning, by establishing new forms of cooperation. The Hub was mentioned as a platform to bring various perspectives together.

Panel 2
INNOVATION IN MONITORING AND SURVEILLANCE

Opening note: Paul Griffiths, *EMCDDA Scientific Director*
Panellists: Teodora Groshkova, *EMCDDA;* Mirela Rogova, *NESTOR;* Antonio Bosisio, *Promenade*
Moderator: Professor Théodore Christakis, *Université Grenoble Alpes*

"The discussions focused on the application of AI, highlighting the importance of investing in innovation.

The Panel focused on effective security solutions while meeting citizens' expectations in terms of privacy, transparency and accountability.
The intervention of Paul Griffiths highlighted current threat areas, including the ability of criminal networks to innovate and exploit new technologies, as well as developments in legitimate business, weaknesses in governance and differences in jurisdictions. The implications for monitoring and surveillance are multiple, but revolve around the need to adapt existing tools to the new challenges, as well as developing new tools and methods. Of crucial importance is our ability to work together, to unite different perspectives in the monitoring and surveillance area, and to build a knowledge community that has a more holistic perspective.
Three presentations followed, displaying innovation in monitoring and surveillance. The EMCDDA presented an innovative approach, applying artificial intelligence to routinely collected data from cannabis resin samples to classify them as originating in Morocco or Europe. This approach has the potential to create novel methods to facilitate international drug monitoring and new insight into the impact of neighbouring countries (such as Morocco) on European drug markets. The flexibility of this approach in adapting to new data and real-world problems could enable it to be applied to a wide range of other contexts in international drug monitoring.
Two EU-funded projects, NESTOR and Promenade, each presented their work, providing examples of new technologies for enhanced surveillance. NESTOR develops a flexible, integrated solution adapted to end users' needs and system requirements. Promenade promotes collaborative exchange of information on vessel position and related information between maritime surveillance authorities, guaranteeing compliance with legal and ethical regulations and norms. The use of AI allows the analysis of large amounts of data by combining it with the use of big data infrastructure to improve border and external security capabilities.
The discussions focused on the application of AI, highlighting the importance of investing in innovation, where legal and ethical assessments are given the highest priority from the outset.

Panel 3
DIGITAL INVESTIGATION TOOLS: FROM RESEARCH TO USE

Opening note: Mailis Pukonen, *CEPOL Head of Operations*
Panellists: Juan Arraiza*, EACTDA;* Anna Illamaa, *ECTEG;* Dr Dafni Stampouli, *Europol Innovation Lab;* Laurent Beslay, *JRC*
Moderator: Michele Socco, *DG HOME*

In her keynote, Ms Pukonen mentioned that criminals already embraced the new technologies and all the advantages offered by the online environment: they can communicate easily, in an anonymous and encrypted way; they can transfer data rapidly from one jurisdiction to another. From the investigative perspective, it is challenging to obtain electronic evidence from other jurisdictions with different legal systems in place. Law enforcement agencies need to have the capacity to identify the needs and prioritise the resources to deliver training and tools in the field of digital investigations. The EU Innovation Hub for Internal Security is an excellent initiative to coordinate such efforts.
In order to help law enforcement agencies to make the most of the opportunities offered by new technologies, and make their job more efficient and effective, the Europol Innovation Lab created the Europol Tool Repository hosting cost-free software tools to help investigators in their daily activities. These non-commercial tools are provided by Law Enforcement Agencies or by Research and Technology Organisations. The tools have been downloaded hundreds of times and have already supported several investigations. Another interesting initiative on Digital Investigation Tools is the FREETOOL Project. It has developed a range of free cybercrime investigation tools tailored to support specific law enforcement requirements in digital investigations and analysis.

Join the **Europol Platform for Experts** (EPE) to learn more about the **EUROPOL TOOL REPOSITORY**

EACTDA (European Anti-Cybercrime Technology Development Association) and ECTEG (European Cybercrime Training and Education Group) are both noteworthy EU funded mechanisms to enhance the framework for the development of new outstanding tools for law enforcement investigators.

The CEPOL Cybercrime Academy will implement various courses covering different aspects regarding digital investigations, in line with the European Multidisciplinary Platform Against Criminal Threats (EMPACT) priorities and training needs of the Member States, and will support other EU funded projects (e.g. AIDA) in delivering training activities on how to use newly developed digital investigation tools.
The creation of free, effective and reliable tools for the support of investigations will greatly assist the fight of all types of crime.
The panellists highlighted the need for a structure to support the entire lifecycle of a project, and a proper evaluation framework to assess new operational tools. Prototypes developed with a research project mind-set are not the same as the end products, e.g. in terms of product security, functionality, software. A decision has to be made whether to invest in further developing prototypes, or to buy off the shelf. More attention should be paid to sustainable outcomes in the calls for proposals and evaluation of funding applications. Funded projects in the area of internal security would benefit from standardised blueprints and procedures.

Eventually, more research closer to operations is required. Training creates a unique opportunity to promote research outcomes. Training on digital skills, especially to extract and handle digital evidence, has been identified as a main core competency gap under CEPOL's EU Strategic Training Needs Assessment.

Panel 4

JUSTICE AND ACCOUNTABILITY:

Visions for the future of Innovation for Security - Investing in sustainable and responsible use of technologies.

Opening note: Luca Tagliaretti, *eu-LISA Deputy Executive Director*
Panellists: Ruth Linden, *AP4AI and Europol Innovation Lab;* Nizar Touleimat, *STARLIGHT and CEA;* Jana Gajdosova, *FRA;* Francesco Contini, *IRSIG-CNR*
Moderator: Professor Matthias Leese, *ETH Zurich*

> ***"We need to define clear use cases where we should or must not use AI in the context of law enforcement and justice.***

In the ongoing digital transformation in the area of internal security and justice, it is vital to ensure the balance between efficiency and accountability, and to guarantee that data will be used in ethical and lawful manner, as identified by the eu-LISA Deputy Executive Director. Data is at the core eu-LISA's business, and the Agency is increasing its contribution in the justice domain with a gradual introduction of new systems to its portfolio: ECRIS, ECRIS-TCN, e-CODEX and Joint Investigation Teams (JITs). eu-LISA is pro-actively analysing the possibilities for the practical implementation of Artificial Intelligence to enhance the digitalization of internal security, including in the justice domain. For instance, a joint report by eu-LISA and Eurojust on "Artificial Intelligence supporting cross-border cooperation in criminal justice" presents several use cases in which AI could support the cross-border judicial cooperation (such as natural language processing, forensic analysis and translations). AI (as any technology) is not a threat by itself - it will not replace humans in decision-making. What needs to be regulated is the way in which AI is being applied, rather than the AI technology itself, and ensure its ethical and lawful use in Europe. A risk-based approach is needed, with a prior assessment of the costs and benefits, fundamental rights and data protection aspects, to determine and guarantee relevant safeguards.

The panel discussion focused on accountability and the responsible use of technologies. Accountability is one of the key principles of the EU Fundamental Rights acquis, whereas the development of new technologies, such as AI, is often focused on improving the efficiency of operations. However, this does not need to result in a conflict between efficiency and accountability.

For example, if an investigation requires face or object recognition on video recordings, multiple false positive results will lead to investigating more people than is necessary and proportionate, where AI can help to increase the accuracy.

Accountability is also one of the key principles of procedural law, and guides every judicial decision. A new challenge consists of finding ways to integrate a non-accountable technology into a system that is based on the principle of accountability.
For that purpose, we need to define clear use cases where we should or must not use AI in the context of law enforcement and justice. Possible areas of less sensitive AI application could be converting speech to text in court proceedings, and automatic translation or assisted analysis of video recordings. Those tools have the potential to make judicial proceedings more efficient, without compromising the accountability principle. However, AI should not be used in the area of predictive justice to support judges in their decisions, as the risks of loss of accountability and independence of the judicial system would clearly outweigh the potential benefits.
Accountability in the digital transformation process can be strengthened by primary legislation (such as an EU AI act); soft law (such as public procurement rules); developing digital tools that are transparent and non-biased by design; and developing digital skills by training law enforcement and justice practitioners. One practical example to support practitioners is the AP4AI project, which has developed accountability principles for the use of AI in internal security via research, consultation with experts and practitioners, and a survey of 6,000 people on their perceptions of AI. The AP4AI principles will be converted into a mobile app to support practitioners in a more practical way, to allow for self-assessment of AI tools, and to provide guidelines on how to improve accountability when using AI. The panellists agreed that the use case is at least as important as the tool itself, and the roles and levels of responsibility of different internal security actors must be taken into account when assessing risk and responsibility.

DAY 1 | TAKE AWAYS

Panellists: Mailis Pukonen, *CEPOL Head of Operations;*
Javier Quesada, *FRONTEX Director ad interim Capacity Building Division;*
Luca Tagliaretti, *eu-LISA Deputy Executive Director;*
Paul Griffiths, *EMCDDA Scientific Director;*
Grégory Mounier, *Europol Innovation Lab, Head of EU Innovation Hub Team.*
Moderator: Nicolas Bessot, *DG HOME, co-chair, Hub Steering Group*

Overall, the agencies are enthusiastic about the Hub's achievements so far: they all committed to increase their engagement and, where possible, their resource commitments.

The Hub was recognised as an important mechanism through which to identify the research needs of the internal security community. Each Hub member operated under different rules and was accountable to different stakeholders, which could make cooperation challenging. However, each JHA agency has its own stakeholder community in the Member States, which can provide invaluable input. Furthermore, the multidisciplinary nature of the Hub allows it to identify 'cross-cutting' technologies, provide a holistic view, and contribute to prioritisation.

A stronger involvement of the EU Member States is envisaged for any future activities.

DAY 2 | ROUNDTABLE SESSION ON ENCRYPTION

The second day of the event saw intense expert discussions on encryption, with a focus on vulnerability management for internal security, the opportunities and impact of quantum computing, innovation on metadata and dialogue with stakeholders. The aim of the session was to address the Hub's tasking from the COSI, but also to go beyond the polarized positions that tend to oppose security and privacy, and to propose an alternative way forward supported by innovations.

Based on two concrete examples of on-going EU projects in the field of encryption, the panellists recommended creating synergies between public authorities and private operators, as well as between law enforcement and judicial authorities of different countries, as the only way forward to combat the cross-border criminal exploitation of encrypted communication platforms. The participants discussed the increasingly critical issue of accessing digital evidence within criminal investigations, while providing the best possible protection for digital systems and fundamental rights; and considered opportunities for innovation.

Possible options included a potential EU vulnerability management policy for internal security and the necessary conditions for its successful development, requiring in particular an appropriate and dynamic oversight mechanism. The participants emphasized the need to adopt a rigorous risk assessment process to implement temporary retention of vulnerabilities and their exploitation by the relevant authorities.

Next, participants presented quantum computing for law enforcement authorities, both as a threat for their cybersecurity and an opportunity for accessing data from criminals. They also underlined the need to explore solutions available today, such as quantum-safe algorithms, which will become useful in the future.

Widening the scope of the challenge of encryption to other key stakeholders, the participants also addressed the possibility of innovating through standardization, highlighting the role of the European Telecommunications Standards Institute (ETSI).
Innovation can also take place in the cooperation with public and private stakeholders, in particular Over-The-Top providers, to access and process metadata without weakening encryption. The panellists underlined the need to support this dialogue with facts and to offer enough transparency to the process while respecting the "space to think" principle.

The experts concluded that the Hub members were ready to support COSI and the Commission in their efforts to address this 'wicked problem', including by preparing a report on innovation and encryption.

Click here to find detailed information on the event, including agenda and speaker profiles