Council of the
European Union

Brussels, 23 September 2022
(OR. en)

12657/22

LIMITE

COSI 235
ENFOPOL 473
CYBER 306
JAI 1228

NOTE

From:	Innovation Hub Team
To:	Delegations
Subject:	EU Innovation Hub for Internal Security - Report from the 2nd Annual Event

Delegations will find attached the Report from the 2nd Annual Event, prepared by the Innovation Hub Team.

ANNEX

EU
INNOVATION
HUB

Shaping Responsible Solutions for Internal Security
EU Innovation Hub for Internal Security Annual Event
in cooperation with the CERIS community

Report from the 2nd Annual Event of the EU Innovation Hub for Internal Security

Context

The EU Innovation Hub for Internal Security (hereafter ‘the Hub’) was created on the instructions of COSI in 2019. The first annual event of the Hub took place virtually in 2021. The Hub Team, hosted by Europol, organised the 2022 annual event of the Hub in collaboration with the Commission DG HOME Innovation and Security Research Unit in Brussels.

Practical Information

Date: 13-14 September 2022

Place: Brussels, Belgium.

Day 1: 4 panels, approximately 100 participants. Main themes: fundamental rights and internal security research, innovation uptake.

Day 2: two project presentations, one roundtable session, approximately 70 participants. Main themes: Quantum cryptography, Vulnerability management systems. Followed by Hub Steering Group informal meeting.

Participants included COSI representatives, JHA counsellors, representatives of EU JHA agencies, Innovation experts from national law enforcement agencies (LEAs), Office of the EU Counter Terrorism Coordinator, Council General Secretariat, European Commission (DG Home and JRC), Czech and incoming Swedish Presidencies, public and private research institutes, industry representatives, Horizon project representatives and civil society organisations. Invitations for day two were more limited to allow for an in-depth discussion.

Event summary – Day 1

Welcome

Nicolas Bessot (Commission DG Home) and Thierry Hartmann (French Ministry of Interior), co-chairs of the Steering Group for the EU Innovation Hub for Internal Security

Keynote

In a pre-recorded address, 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 COSI. He highlighted the relevance of the Hub's pilot projects, in particular the Accountability Principles for Artificial Intelligence (AP4AI). He encouraged 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

Panel opening: Michael O'Flaherty, FRA Director (pre-recorded)

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

Opening the Panel, 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, he expressed the view that fundamental rights compliant security strategies are better strategies that make us more secure. He pleaded to keep in mind not only respect for privacy, but also potential chilling effects for all the other fundamental rights, including, for example, non-discrimination, the freedoms of expression, assembly and movement. Mr O'Flaherty referred to three elements of legality, necessity and proportionality, which need to be respected for any limitation on fundamental rights to be justified. He said that fundamental rights compliance had to be assessed at different stages: in the design of the technologies, in the training of the technologies, in the operation of the technologies, and following their application. He also stressed the importance of strongly embedded oversight authorities to ensure a full respect for fundamental rights. In conclusion, he expressed the hope that the discussion on fundamental rights would be mainstreamed throughout the entire conference.

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

Panel opening: Paul Griffiths, EMCDDA Scientific Director

Panellists: Teodora Groshkova, EMCDDA; Mirela Rogova, NESTOR; Antonio Bosisio, Promenade

Moderator: Professor Théodore Christakis, *Université Grenoble Alpes*

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, showcasing 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

Panel opening: 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 the 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.

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 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 following points:

- There is a 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 something from the market.
- There has to be more research closer to operations. 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.
- More attention should be paid to sustainable outcomes in the calls for proposals and evaluation of funding applications.
- Funded projects in this area would benefit from standardised blueprints and procedures.

Panel #4: Justice and Accountability: Visions for the Future of Innovation for Security – towards Responsible Use of Technologies

Panel opening: 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

Mr Tagliaretti used his address to reflect on the responsible use of technology, referring to some of the main large scale IT projects current underway in relation to judicial cooperation, such as ECRIS-TCN. He announced that a digital platform to support Joint Investigation Teams (JITs) should be delivered by 2026.

The panellists compared their experiences in different projects and agencies. AP4AI showed the importance of the citizen perspective: data collection showed that citizens' trust in law enforcement processes was relatively high.

Given that AI relies on probability, users of such systems need to have a proper understanding of what they are using. The use of AI systems touches on several fundamental rights and related concept. The cross-fertilisation between various EU-funded projects was highlighted. The panellists also noted that future AI legislation would apply equally to all software, whether developed 'in house' or procured commercially. Therefore, internal procedures would have to consider how to ensure the compliance of tools developed by other parties. 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.

Closing remarks

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.

Event Summary – Day 2

Roundtable Session on Encryption

Themes:

- Vulnerability Management for Internal Security
- Quantum Computing: Opportunity and Impact
- Innovation on Metadata and Dialogue with OTT

Panellists: Louise Hachin and Olivier Zheng, French Gendarmerie; Driss Aboulkassimi, CEA; Laurent Beslay, Commission Joint Research Centre; Sven Herpig, *Stiftung Neue Verantwortung*; Nico van Eijk, CTIVD; Iwen Coisel, Europol European Cybercrime Centre (EC3); Elham Kashefi, University of Edinburgh/CNRS; Jean-Christophe Le Toquin, Encryption Europe; Markus Keil, *Bayerisches Landeskriminalamt*.

Moderator: Emmanuel Saliot, Council of the EU.

The Hub dedicated the second day of its annual event to the topic of encryption, in order to address the Hub's tasking from the COSI, but also in order to go beyond the polarized positions that tend to oppose security and privacy, and to propose an alternative way forward supported by innovations.

This session was introduced by Boštjan Škrlec, Eurojust Vice-President, who addressed some of the main critical areas in the field of criminal investigations and prosecutions associated with encryption. Mr Škrlec 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 session aimed at addressing the increasingly critical issue of accessing digital evidence within criminal investigations, while providing the best possible protection for digital systems and fundamental rights. The participants considered the following questions:

- How can progress be made to tackle the constraints on law enforcement and justice created by encryption, without creating additional risks for fundamental rights or the legitimate protection of information?
- Which are the innovation domains where a consistent approach to encryption under this objective is essential?

The session offered two concrete examples of on-going EU projects in the field of encryption. Building on the insights provided in the presentations, the panellists explored three possible approaches to encryption.

The discussion started with the opportunity of a possible EU Vulnerability Management policy for Internal Security and the necessary conditions for its successful development, in particular appropriate and dynamic oversight mechanism. The participants emphasized the need to adopt a rigorous risk assessment process in order 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 ETSI. Innovation can also take place in the cooperation with public and private stakeholders, in particular Over-The-Top providers, in order 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 conclusion of the day’s discussions on encryption was that the Hub members were ready to support COSI and the Commission in their efforts to address this ‘wicked problem’, for example by preparing a report on innovation and encryption.

Informal Steering Group Meeting

The annual Hub event was immediately followed by an informal meeting of the Hub Steering Group, to which all members of the Hub Team were also invited.

Steering Group members agreed that the event had demonstrated the ability of the Hub to bring together experts from a wide variety of professional fields in order to make progress in exploring complex yet important topics.

Member State representatives expressed the wish that national needs and priorities should be reflected in the work of the Hub. The Steering Group agreed that this could be achieved through the mapping exercise that is nearing completion, as well as by hosting Member State representatives in the Hub Team (noting that France already seconded a national expert to the Europol Innovation Lab to work on some Hub-related projects). The Steering Group also agreed that the Hub's activities could benefit from greater visibility at Member State level.

The Steering Group agreed in principle to hold a formal meeting before the end of 2022 in order to discuss the findings of the mapping exercise.