EU INNOVATION HUB

EU Innovation Hub for Internal Security

Annual Event Report 2023

EU INNOVATION HUB FOR INTERNAL SECURITY ANNUAL EVENT
in cooperation with the CERIS community

Brussels, 3 October 2023

The EU Innovation Hub for Internal Security (the 'Hub') is a cross-sectoral EU platform which aims to ensure coordination and collaboration between innovation actors in the wider field of internal security. The Hub, composed of various EU Justice and Home Affairs agencies, the European Commission (DG HOME and DG JRC), the General Secretariat of the Council including the EU Counter-Terrorism Coordinator's Office, 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 click here.

EU INNOVATION HUB ANNUAL EVENT REPORT 2023

PDF | ISBN 978-92-95236-29-5 | DOI: 10.2813/866510 | QL-09-24-257-EN-N

Luxembourg: Publications Office of the European Union, 2024

Cite this publication: Europol (2024), EU Innovation Hub Annual Event report 2023, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu

EU INNOVATION HUB FOR INTERNAL SECURITY

HIGH-LEVEL OPENING

The co-chairs of the EU Innovation Hub Steering Group, Enrique Belda-Esplugues, Deputy Director General of Communication and Information Systems for Security and Director of the Security Technology Centre, Ministry of the Interior, Spain, and Nicolas Bessot, Head of the Innovation and Security Research unit, Directorate-General for Migration and Home Affairs, European Commission, opened the high-level session by underlining the strategic importance of the EU Innovation Hub for Internal Security (the 'Hub') and its relevance for end-users in the EU Member States.

The high-level panel composed of senior representatives of the Hub membership discussed the significance of innovation in the wider field of EU internal security.

Agnès Diallo, Executive Director of eu-LISA, praised the Hub as a platform for addressing issues that individual actors cannot solve on their own. For eu-LISA, biometrics and Artificial Intelligence (AI) are relevant topics for the Hub. The Hub's role in strategic foresight should be further explored, not least by leveraging the depth and breadth of the Hub's network to bring information to key decision-makers.

Montserrat Marín López, Executive Director of CEPOL, linked innovation with education, aspiring to keep up with new technologies such as AI. Improving knowledge management within the Hub was equally high on CEPOL's agenda.

Aija Kalnaja, Deputy Executive Director of Frontex, spelled out her vision for the Hub, including continuous learning, directing research, and deploying results to the field. Capability roadmaps, already familiar in the defence sector, could be used more in the internal security community.

Andrei Linta, Deputy Executive Director of Europol, acknowledged the need to accelerate innovation in internal security and recognised the Hub's unique position in the EU's internal security landscape to do so, with a direct benefit for the Member States.

Marta Cygan, Director in the European Commission's DG Migration and Home Affairs, commended the direct engagement of the Hub with practitioners, as well as with the CERIS community, bringing together policy-makers, researchers, industry representatives and operational experts. Research and innovation gaps identified by this community should translate into projects funded by the EU's 'Horizon Europe' funding programme, with the Hub having a distinct role in the dissemination and uptake of those projects.

Panel 1
Key enabling technologies

Panellists:

- Isabel Praça, Professor at the Instituto Superior de Engenharia do Porto and Senior Researcher in the Research Group on Intelligent Engineering and Computing for Advanced Innovation and Development (GECAD)
- Isabelle Linde-Frech, Head of Business Unit Public Technology and Innovation Planning, Fraunhofer INT
- Seán Gaines, President of the Board, European Anti-Cybercrime Technology Development Association (EACTDA)
- Christian Bratz, Assistant Director Strategic Innovation, Interpol

Moderator: Darek Saunders, Head of Border Security Observatory a.i., Frontex

The panel discussion was centred on increasing awareness about key enabling technologies (KETs), highlighting their potential to significantly strengthen the EU's technological capabilities in internal security. The discussion delved into ways of enhancing the EU's technological sovereignty in this area.

The discussion included insights from Interpol, detailing its efforts over the past decade at the Interpol Global Complex for Innovation (IGCI), particularly in innovating KETs. The key initiative mentioned was the use of AI in law enforcement in a responsible manner, leading to the development of a toolkit in collaboration with the United Nations Interregional Crime and Justice Research Institute (UNICRI), funded by the EU. The conversation also touched on the Playbook for a holistic law enforcement approach to emerging technologies, a critical part of Interpol's strategy.

The focus then shifted to the application of AI in the realm of cybersecurity. The panel explored how AI tools are currently employed to analyse vast datasets to identify cyber threats and the potential of AI to fill the talent gap in cybersecurity. The importance of protecting AI systems in internal security, the risks associated with AI tools, and the need for explainability in AI systems were also discussed. Emphasis was placed on the need for continued investment in AI research and the development of skills, particularly concerning the security of AI systems.

From the Fraunhofer perspective, with extensive experience in defence technology, the panel discussed the overlap and differences between technologies for defence and civil security. The panel highlighted the 'top trends' in technology foresight, including challenges in post-fossil energy supply, bio-technical convergence, and various AI aspects such as virtual command and control solutions and human-robot interfaces.

The panel also addressed the sensitive nature of data, which makes pooling resources for shared AI solutions difficult and is therefore a significant challenge. Federated learning was suggested as a viable solution, allowing for the combination of insights from various law enforcement agencies without the need to share the data itself.

A key takeaway from the panel was the underutilisation of many KETs by internal security practitioners, often due to the need for customisation to specific operational contexts and existing regulations. Early identification of these needs in the R&D process and a systematic approach to understanding how new solutions fit within existing technological frameworks and systems were deemed essential.

Panel 2
Regulatory sandboxes

Panellists:
- Martin Übelhör, DG HOME F2, Innovation and Security Research, European Commission
- Jennifer Woodard, Co-founder, Insikt Intelligence, and Member of the CERIS Expert Group
- Petr Motlicek, Idiap Research Institute and Brno University of Technology, Member of the CERIS Expert Group
- Eirik Gulbrandsen, Norwegian Data Protection Authority

Moderator: Dr Dafni Stampouli, Europol Innovation Lab

Article 53 of the Proposal for an EU Artificial Intelligence Act envisages setting up coordinated AI 'regulatory sandboxes' to provide a controlled environment that facilitates the development, testing and validation of innovative AI systems for a limited time before placing them on the market or putting them into service. In the field of law enforcement, a sandbox can allow developers and innovators to test, experiment and develop their ideas and co-create solutions, ultimately leading to better outcomes for their projects and operational law enforcement tasks. In line with its amended Regulation (EU) 2022/991, Europol is currently developing such a sandbox for law enforcement.

The panel discussed what is considered a game-changer for the internal security community, not least against the background of the Commission's preparation of a European Security Data Space for Innovation.

The draft EU AI Act is intended to establish safeguards, using a risk-based approach. At the same time, it also aims to promote the EU's digital sovereignty by encouraging innovation originating in the EU and by making available high computing capacities to SMEs. Sandboxes, to be set up in cooperation with competent authorities, are considered a building block of this approach, providing a controlled environment for testing, in full compliance with the obligations of the future AI Act. The draft legislation, clarifying the safeguards, was welcomed from an SME perspective. 'Safeguarding' and 'trustworthy AI made in the EU' as a business model could even turn into a competitive advantage. The experience in Norway showed the need for a more permanent sandbox environment for the development of responsible and privacy-friendly AI. The Norwegian data protection authorities' optimistic view on AI contributes to finding solutions, inter alia by changing the respective business models into a joint responsible processing of data, with a focus on how the data is used in a specific project, and for which the sandbox is instrumental in proving fairness and explainability, and the robustness of a model, all of which ultimately work in favour of the consumer.

From a technical perspective, the panel underlined the role of sandboxes in increasing the performance and accuracy of models in a fast-paced environment. The question of explainability is increasing in complexity, in particular for large language models. In the future, the focus might shift from showing how a particular model was trained to rather how a decision was taken, including tracing back from which data sources the model has learned instead of trying to understand what the model actually does.

Sandboxes will also play an important role when addressing the currently unresolved matter of how to replicate results. In the field of justice and home affairs, reproducibility will be indispensable for the use of AI tools for evidence in court proceedings. However, the use of a sandbox would not guarantee the conformity of products that exit such a sandbox and should thus not be presumed.

Instead, performance criteria are needed for projects that 'graduate' from a sandbox. In any case, such graduation cannot be more than a snapshot in time, as models keep on learning and thus change over time.

The panellists identified the limited access to relevant data as an impeding factor for the successful use of sandboxes. However, each sandbox would not require its own individual data infrastructure. Instead, the Commission is currently undertaking steps to set up an environment to train and test AI models in the field of justice and home affairs: a study had just been completed on a future EU Security Data Space for Innovation. Europol's sandbox could become the first main building block of the future space, as well as a data resource.

The discussion evolved further around the balance between necessary innovation and ensuring compliance of results.
A collaborative approach during the entire project lifecycle was valued, as well as the need for supervision after the completion of a project, with a view to solving similar problems before other projects face them. Some obligations will be regulated by law, but trust is generated by a combination of various aspects, including transparency, standards, documentation and human oversight. Continuous communication remained a highly underestimated part of the work of project teams and supervising authorities alike.

Overall, both regulatory and business learning were considered essential for the success of sandboxes, along with solid AI expertise on all sides, including among regulators. For such learning to be implemented, more use cases would be beneficial.

Panel 3
Encryption & access to data

Panellists:
- Dr Jurjen Jansen, Cybersafety Research Group
- Peter Alexander Earls Davis, University of Copenhagen
- Ferre Pauwels, Belgian Federal Ministry of Justice

Moderator:
Laurent Beslay, DG Joint Research Centre, European Commission

The panel focused on the challenge of accessing encrypted metadata and content data for investigative purposes. Tackling this challenge requires not only technological innovation, but also innovative approaches to the regulatory framework, data protection and judicial proceedings.

The Dutch Police Academy opened the session with a presentation of a project focusing on the role of encryption in police investigations when used by criminals for communications, devices and data, tools hiding digital locations (e.g. VPN) and encrypted online services. Encryption is a challenge for law enforcement authorities on a daily basis, in particular when investigating subversive and high-impact crimes, such as drug-related crime, child sexual exploitation and cybercrime.

The impact of encryption on the pace of investigative work is extremely high, with investigations requiring months or years instead of weeks, or being dropped entirely due to the inability to access evidence. At the moment, investigators have only limited options: cracking encryption or bypassing it by finding the encryption key, guessing the key, enforcing the key, exploiting a leak in the encryption software, gaining access to readable text when using the device, or locating a copy of the readable text.

The results of the research project suggest that access to encrypted data helps with direct access to evidence in a timely manner, significantly aiding the investigative work.

However, there are examples of successful investigative work even when encrypted data could not be accessed, with the help of metadata and other non-digital methods. In addition, access to encrypted data will not necessarily result in successful investigation, as encrypted data may contain no relevant evidence. A holistic view is therefore needed to get to the core of the 'problem' of encryption.

The panellists also discussed the importance of innovating within the existing regulatory framework. Today, criminals exploit four layers of 'going dark': main communication service providers; niche providers (e.g. crypto-phones); Virtual Private Networks (VPNs), The Onion Router (TOR) or Tails (a browser that uses TOR); and other ways that do not rely on encryption (e.g. burner phones, gaming chats, etc.). Design mandates for backdoors are not realistic, so there is a need to explore other innovative approaches.

A low-hanging fruit for regulators may be innovation in legal approaches. Another option is innovation in organisations (e.g. the new EU Child Safety Agency, which could act as a trusted broker between service providers and law enforcement)

or interorganisational cooperation (e.g. the 'Trojan Shield' or 'Greenlight' operations, both supported by Europol). Innovation in research is also important, including comparative research looking at the use of encryption and its regulation in fields other than criminal investigations (e.g. regulating actors using encryption rather than regulating encryption as such).

Finally, it is important to consider innovation in public discourse, focusing on encryption, to tackle the issues of oversimplification or polarised debates juxtaposing privacy and security.
The panel closed with a discussion on the challenges for legislators to address the issue of encryption appropriately.

The debate is currently dominated by single-issue campaigners, such as privacy advocates and NGOs, big tech companies, judges, and law enforcement authorities. It is very difficult, if not impossible, for legislators to satisfy the expectations of all these groups. In the Belgian legal system, service providers have the obligation to cooperate when a judge issues a warrant; however, this obligation on providers to decrypt is unenforceable as they do not necessarily have the means to do so.

The Belgian Data Protection authority's position is that government authorities, including law enforcement, could rely on intrusive tools as a first-order choice, before introducing additional legal means to require providers to share data with law enforcement. This position is not clear to law enforcement authorities. To tackle some of the challenges related to encrypted data, providers of encrypted communication services should come up with solutions.

Panel 4
Bridging the valley of death: ensuring the uptake of outputs of EU security research

Panellists:
- David Rios Morentin, Vicomtech
- Jorge Garzon, French Ministry of the Interior
- Eleni Lianou, KEMEA
- Hans-Martin Pastuszka, Fraunhofer INT

Moderator: Ana Lucia Jaramillo, Corvers

The panel on the uptake of results of security research projects funded by the EU focused on a range of factors affecting the uptake, including market fragmentation, end-user involvement, intellectual property rights and funding.

In their opening statements, panellists highlighted the fact that a lot of work has been done to understand what works and what does not, providing a solid basis for further improvements; however, a number of challenges remain. First, the EU security market is highly diverse and fragmented, far more fragmented than the markets in the areas of defence or space. Therefore, there is a need to identify or develop best practices on how to approach and engage with the market. Second, it is important to understand the value chain and enter the value chain as early as possible, in order to maximise the utilisation of research results. A number of actions can be taken to address this, including: shifting the focus of security research programming from scientific to operational impact; improving the sequential planning of inter-related projects to better fit with the value chain, and making the value chain more visible, transparent and reliable.

Finally, better understanding the actors involved and their needs, and planning EU-funded research and innovation projects to address those needs (e.g. focusing on innovation actions with higher TRLs, and pre-commercial procurements) may help improve research uptake.

Continuing the discussion, the panellists covered some of the factors in detail. Addressing market fragmentation, they suggested that economies of scale can be gained through joint cross-border public procurement (JCBPP). However, the success of JCBPP depends on a number of factors, including the standardised definition of needs, as well as training and awareness activities, and involvement of a high number of end-users in the definition of needs, as well as in the deployment planning. With regard to funding, it is important to address the diverse financial capacities and planning cycles across the Member States.

EU funding can facilitate this to a certain extent, by lowering the financial burden for some Member States. In addition, making the links between different funding instruments more transparent would help in ensuring continuity. In that sense, linking the Internal Security Fund and the Border Management and Visa Instrument with relevant parts of the Horizon framework would facilitate the uptake of research results.

In closing, focusing on de-risking innovation procurement, panellists emphasised the importance of thinking in terms of value chains, and identifying the potential risks at the beginning of the process. Foresight activities and capability roadmaps would help in the risk identification, as well as in building consensus between the demand and supply sides.

TAKE AWAYS

The Hub Steering Group co-chairs concluded the event by underlining the importance of sharing and standardising in the EU, aiming at creating an innovation-friendly environment which helps to overcome the obstacles that the entire community is currently facing. It was considered important to enlarge this discussion beyond the EU internal security institutions and agencies to raise awareness and increase cooperation with the wider community, including academia and industry. The co-chairs called upon all actors to play their role in making Europe fit for the digital age.