Council of the
European Union

Brussels, 27 March 2024
(OR. en)

7745/24
ADD 1

LIMITE

COSI 47
ENFOPOL 154
CYBER 100
JAI 537

NOTE

From:	EU Innovation Hub
To:	Delegations
Subject:	EU Innovation Hub for Internal Security - Work plan 2024

Delegations will find attached the work plan 2024, endorsed by the Steering Group of the EU Innovation Hub in March 2024.

12 February 2024

#1350677v19

EU Innovation Hub for Internal Security

Work Plan 2024

Addendum to the Multi-annual planning of activities 2023-2026

Complementing its Multi-annual planning of activities 2023-2026[1] and indicative planning matrix 2024-2026, the EU Innovation Hub for Internal Security ("Hub") is proposing detailed activities to be carried out in 2024 in this Work Plan.

Following the outcome of the Hub Steering Group meeting of 4 October 2023[2], the Hub Team is proposing to carry out its activities in thematic clusters, as specified in chapter I of this document.

A thematic cluster is defined as a thematic priority for the Hub in which individual Hub Team members agree to work collaboratively with one of them being in the lead. The cluster leader will drive the work in the area while respecting the autonomy of the Hub members carrying out activities within the cluster, and report on the progress and results of activities on a regular basis to the entire Hub Team. All clusters will engage with relevant Horizon Europe and other EU or MS funded projects to ensure information flow about topical developments and engage with them as appropriate. The cluster topics and activities might be updated during the year if needed, reflecting the agile EU internal security innovation environment.

1 5603/23
2 1342312

Beyond the thematic clusters, the Hub Team continues to work jointly on several topics of interest related to innovation in the field of EU internal security, as well as on events. An indicative list, which might be revised during the year, is presented in chapter II of this document.

I. EU Innovation Hub thematic clusters

A) Foresight and key enabling technologies

Lead: DG HOME

Members: CEPOL, DG JRC, EMCDDA, eu-LISA, Europol, Frontex

Activities:

a) Mapping of Key Enabling Technologies. Key Enabling Technologies (KETs) should be understood as technologies, which alone or in combination with other technologies have the potential to significantly enhance or deliver new capabilities. The purpose of the cluster is to map such technologies relevant for security and border management, discuss ways to strengthen the EU's technological sovereignty in KETs and present how some of those technologies could enhance the EU capability portfolio.

b) The cluster will also contribute to the better understanding of foresight methodologies and forward-looking capability development planning.

c) Critical technology dependencies in civil security and border management will be assessed.

d) Technology scanning will be conducted in some case studies. For example a case study proposed by EMCDDA relates to drug markets.

e) The cluster can assess the outcomes of the AHEAD project (TowArd TecHnological ForEsight for IncreAseD Security) and make use of the project's main outputs as well as the prospective foresight methodology.

B) Biometric recognition systems: data quality, evaluation and standardisation

Lead: eu-LISA

Members: DG HOME, DG JRC, Europol, FRA, Frontex

Rationale:

EU Agencies (e.g. eu-LISA, Europol, Frontex) as well as Member State (MS) authorities rely on biometric technologies (ABIS/AFIS, etc.) provided by commercial vendors. Although vendors are required to provide performance evaluation results, at the moment EU Agencies and MS authorities have limited ability to perform independent testing/performance evaluation of biometric recognition systems (with the exception of a few laboratories in some MS that can provide such services). At the moment most EU actors rely on the US National Institute of Standards and Technology (NIST) to perform independent evaluation of biometric recognition systems; however, it is unsure whether the systems and algorithms assessed by NIST are the same as acquired by some of the EU Agencies and/or MS authorities. The lack of capability to perform independent assessments has implications for the strategic technological autonomy of the EU, which is one of the priorities of the Commission. Additionally, this lack of capability to conduct independent assessments may become an issue with the entry into force of the EU Artificial Intelligence Act.

The current lack of a biometric evaluation capability at EU level described above, stems primarily from the scarcity of large-scale biometric data sets that can be used in such assessments, which is compounded by the lack of an authority that could take on the responsibility for such independent assessments and provide this as a service to the EU.

Insofar, the initial objective of the cluster for the first two years after its creation will be to carry out specific and targeted projects in the field of biometric algorithm evaluation and of biometric quality estimation. These targeted studies should provide detailed evidence and input for the improvement in the management of large-scale IT systems at EU level, and to the standardisation of biometric technology.

Activities:

Considering the challenge indicated above, the cluster will initially focus on the following activities:

a) Maintenance and evaluation of the Open source Face Image Quality (OFIQ) – vendor-agnostic algorithm for the assessment of face image quality developed by the German BSI[3].

b.1) Contribution to the development of a standard (ISO/IEC) for finger-mark (latent fingerprint) image quality.

b.2) Development of a software open-source quality measure for finger-marks aligned with the ISO/IEC standard. Evaluation of existing quality measures for finger-marks.

c) Evaluation of biometric recognition systems, especially with regard to the variability of their accuracy related to demographic features such as age, gender or ethnicity.

d) Study on Remote Biometrics Identification in Law Enforcement (FRA)

To kick-off the work of the cluster, eu-LISA will organise a workshop for the members of the cluster, involving biometrics experts from each of the agencies/institutions.

In addition to the core activities outlined above, the cluster will provide a regular (e.g. quarterly) forum to discuss other pertinent issues in the area of biometric recognition identified by the members of the cluster, and engage with EU-funded projects in the field as appropriate.

[3] Bundesamt für Sicherheit in der Informationstechnik – German Federal Office for Information Security

C) Artificial Intelligence (AI)

Lead: Europol

Members: CEPOL, DG HOME, DG JRC, EMCDDA, EUAA, EU CTC's office, eu-LISA, Eurojust, FRA, Frontex

Activities:

a) AP4AI/CC4AI:

Led by Europol and CENTRIC[4], with contributions and validation from Hub Team members (CEPOL, EUAA, eu-LISA, Eurojust, FRA), the AP4AI project developed accountability principles for internal security over the last three years5. The project developed solutions to assess, review and safeguard the accountability of AI usage by internal security practitioners in line with EU values and fundamental rights. AP4AI means a step-change in the application of AI by the internal security community by offering a robust and application-focused Framework that integrates security, legal, ethical as well as citizens' positions on AI.

In view of the upcoming implementation of the EU AI Act, Europol is now leading the development of a web-based tool to help internal security practitioners to assess the compliance of their AI systems with the requirements of the EU AI Act. CC4AI (compliance checker for AI, building on AP4AI) will allow users to evaluate whether existing or future applications meet the requirements set by the new regulatory framework. The functionality and content of the tool is being developed in consultation with the Hub members active in this field. Access to CC4AI will be offered freely to internal security agencies, and the Hub can play a fundamental role in the validation, roll out and promotion of the tool.

4 A research body at Sheffield Hallam University
5 Accountability Principles for Artificial Intelligence: ap4ai.eu

b) EU Security Data Space for Innovation:

In 2022, DG HOME commissioned a feasibility study from EY[6], examining the technical, legal and financial conceptualisation of an EU Security Data Space for Innovation (EU SDSI). The objective of the study was to improve the EU-wide sharing of, as well as access to, a sufficiently high quantity of high-quality data, as an enabler and catalyst for the development and application of AI and other technologies in the field of Justice and Home Affairs.

The envisaged EU SDSI is meant to enable EU Law Enforcement Agencies and other actors to develop, test and validate their digital tools.

As to the planned design of such an EU SDSI, the study recommends an efficient, federated IT platform through which EU level and national LEAs can collaborate in the area of data driven innovation based on both specific use cases and shared principles and processes. Depending on DG HOME's final decision on the design of the data space, the Hub could be instrumental in supporting the further conceptualisation and implementation of the project. The Hub could establish a dialogue with any project resulting from a recent ISF call published by DG Home in this regard[7].Future Commission efforts towards a SDSI will build on the "Europol Sandbox".

c) The cluster should also engage with relevant EU-funded and other projects exploring AI-related use cases in particular with the project *TESSERA: 'Towards data sets for the European Data Space for Innovation',* coming from the call: ISF-2021-TF1-AG-DATA - data sets for the European Data Space for Innovation. This project will start on 1 March 2024 and will focus on complementing the European Security Data Space for Innovation, as one of the major elements in DG HOME's strategy to increase trust in the use of Artificial Intelligence by law enforcement, by defining and preparing national components for the data environment for innovation to improve the access of national LE authorities to high-quality and high-quantity data to test, train and validate algorithms. The definition and creation of relevant datasets will be based on identified operational use-cases.

---

6 Report: https://data.europa.eu/doi/10.2837/618398
Summary: https://data.europa.eu/doi/10.2837/575135

7 ISF-2021-TF1-AG-DATA; project start expected for March 2024

d) CEPOL research project on AI targeting law enforcement training: in line with article 5 of the CEPOL Regulation, CEPOL will interact with the cluster members when developing the project, which will conduct research in order to inform the design of learning and capacity building activities at a later date.

D) Encryption

Lead: DG JRC

Members: DG HOME, eu-LISA, Eurojust, Europol, FRA, GSC

Activities:

a) Encryption Observatory Report: Europol, Eurojust, eu-LISA, DG HOME and DG JRC will be finalising the fourth edition of the EU Joint Observatory Function Report on Encryption, with a focus on innovation. Publication is envisaged for Q1/2024.

b) Follow up on the relevant recommendations deriving from the outcome of the High-Level Group (HLG) on access to data for effective law enforcement. Engage with encryption-related EU funded projects as appropriate.

c) Post quantum encryption:

One of the main recommendations of Europol's recent report "The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement"[8] is that EU law enforcement should urgently start auditing their communication and storage systems to make sure that the cryptographic protocols they are relying upon for secure communication and storage of sensitive information are post-quantum safe. Europol suggests raising awareness about this imminent threat in the wider internal security community, including at the EU political level and calling for all authorities to invest in a transition plan.

[8] https://www.europol.europa.eu/publication-events/main-reports/second-quantum-revolution-impact-of-quantum-computing-and-quantum-technologies-law-enforcement

d) Explore future opportunities of quantum computing for Internal Security, providing a new level playing field for investigation capability and digital forensic practices.

e) Vulnerability management: DG JRC intends to organise a workshop with DG HOME and the other cluster members aiming at identifying best available techniques for the management of vulnerabilities in the field of Internal Security.

II. EU Innovation Hub Horizontal Activities

E) Knowledge management and innovation in training

Lead: CEPOL

Members: DG HOME, eu-LISA, Europol

Activities:

a) Create within CEPOL's LEEd a knowledge platform for the Hub members' interaction with the forum, innovative contents and announcements on research.

b) Conduct internal surveys for subsequent needs analysis, aiming at organising research or innovative training sessions for the Hub members (platform discussion).

c) The European Law Enforcement Research Bulletin is being reorganised into thematic areas (Environmental crime, Human trafficking, Public Order, etc.). The activities organised under the publications umbrella will target scientific publications, the thematic topics intertwined with innovations, interaction with the CEPOL Board of Editors. It will also potentially channel the organisation of thematic numbers under the cluster thematic areas, opening an organised visibility for the Hub thematic clusters. The Hub members are invited to contribute with articles to the special edition on Environmental Crimes (planned to be issued in June 2024) and Trafficking in Human Beings (planned to be issued in October 2024) and/or by suggesting other contributors to the specific thematic editions or to the generic online version of the Bulletin.

d) Develop law enforcement training: Different innovative training methodologies, tools, projects or ideas will be open for discussion and channelled through the best ways to contribute to increase the capacity of training. Specifically, Hub members are invited to actively participate in a working group planned to start its activities in September 2024.

e) Boost the idea of networking: Different networks will be put in contact with each other, allowing the establishment or reinforcement of contacts between the Hub members and different scientific/research groups. The first initiative is planned on 5-7 June 2024 at CEPOL to network with the EU-ANSA[9] network (scientific programme to be prepared, probably on foresight and key enabling technologies).

f) "Train the trainers": One spot made available for one of the Hub members to participate in the CEPOL "train the trainers" in 2024 (date to be confirmed between May-July 2024) A to allow the Hub to have increased capacity to communicate;

g) Involvement in science and research: Provide the Hub members access to different discussion fora targeting science and research to benefit from the expertise of each Hub member to increase the quality of the outcomes, but also enriching the Hub as a forum of expertise. One parallel session in the annual conference on High Risk Criminal Networks to be organised (date to be confirmed, 16-18 October or 20-22 November 2024) could be organised for the Hub.

Involve the Hub in the upcoming CEPOL Strategic Training Needs Analysis exercise in 2024. One of the Hub meetings during Q3/ 2024 to be organised to collect the insights/opinions/feed-back of the EU-Innovation hub members on the different reports organised by CEPOL.

F) Other Topics of Interest

The Hub's Multi-annual planning 2023-2026 included, for the indicative planning, in addition to those already mentioned in the above clusters, also the following topics:

- secure communications,
- drones,
- virtual/extended reality,
- metaverse,
- privacy-enhancing technologies.

[9] EU Agencies Network on Scientific Advice

Those topics remain areas of interest of the Hub but will not be treated as a priority in 2024. In the case of privacy enhancing technologies, the Hub should consider the conclusions of the Hub study launched in 2023 (funded by Frontex) and reflect on the need for further activities.

G) Events

– Annual event: In 2022 and 2023, the Hub team organised a Hub annual event in Brussels with Commission funding. While both events were very positively evaluated, they also required significant resource investment from the Hub team. The Hub Team is looking into organising a similar event under similar conditions in 2024.

– Strategic retreat for the senior leadership of Hub members: in 2019, the so-called THE CAMP high-level meeting, organised by the EU Counterterrorism Coordinator, became instrumental for the creation of the EU Innovation Hub for Internal Security. In 2024, the Hub Team will explore the appetite for a similar event among senior management Hub stakeholders with a view to organising a follow-up meeting, potentially in 2025.