Council of the European Union

Brussels, 21 November 2022
(OR. en)

14695/22

LIMITE

COSI 288
ENFOPOL 555
CYBER 362
JAI 1460

NOTE

From:	Innovation Hub Team
To:	Delegations
Subject:	EU Innovation Hub for Internal Security: Mapping of common innovation picture in the EU and the EU Member States - Report

Delegations will find attached the report regarding the Mapping of common innovation picture in the EU and the EU Member States, prepared by the Innovation Hub Team.

EU Innovation Hub for Internal Security

Mapping of common innovation picture in the EU and EU Member States

Report

Table of Contents

1. Introduction

The EU Innovation Hub for Internal Security (the Hub) is a collaborative network of innovation labs that was endorsed by the Ministers of Home Affairs in December 2019 and, subsequently, established by the Council's Standing Committee on Operational Cooperation on Internal Security (COSI) in February 2020. The EU Innovation Hub is a cross-sectorial EU platform and aims to ensure coordination and collaboration between all innovation actors in the wider field of the internal security. The Innovation Hub, being composed of various EU Agencies, European Commission (including JRC), the Council General Secretariat and the Office of 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.[1]

Among other tasks assigned to it by COSI[2], the Hub is responsible for assessing gaps and needs and knowledge management for innovation in the field of EU Internal Security. COSI asked the Hub to collect information about key innovation actors and projects in both the EU and its Member States (MS). As specified in the Hub's annual report 2021, the objective includes the establishment of a "*common innovation picture for internal security by*

- *mapping existing and future projects to foster synergies and optimise the use of resources in a decentralised manner with contributions from all Agencies/sectors,*
- *assessing gaps and needs in key areas of relevance for security practitioners and preparing an overview of these gaps and needs, relying on input from all Agencies/sectors,*[3]

---

1 For more information on the Hub, please refer to: https://www.europol.europa.eu/operations-services-innovation/innovation-lab/eu-innovation-hub-for-internal-security

2 5757/20, p. 3; 7829/20, p. 3

3 COSI, The EU Innovation Hub for internal security - Draft operational and financial models, 18 May 2021, WK 6558/2021, p. 5.

– *linking these summarised security related innovation needs beyond the area of JHA into the broader context of strategic and political discussion, via DG HOME into the Commission, and via the Council General Secretariat and the EU Member States into the Council,* […] *and*

– *map and regularly update possible funding instruments for innovation, with the support of the European Commission,*[4] *at EU level, as well as at the level of and with input from individual Member States.*"[5]

For COSI, this mapping exercise is considered a priority for the Hub in 2022.[6] The resulting document is meant for distribution in COSI, after approval by the Hub Steering Group on 9 November 2022.

2. Methodology

With a view to fulfilling the expectations expressed by COSI, in spring 2022, the Hub Team jointly developed:

– a stakeholder map for each Hub member, listing its key stakeholders (MS key contact points, networks, projects, Agency contacts, academia, Research and Technology Organisations, private partners)[7]; and

– a *questionnaire* to be distributed to those communities.

Once the content was agreed, the questionnaire was uploaded to the EU survey tool for easy distribution to the respective stakeholder communities. The questions included, inter alia: nature of responder, project description or importance of the projects, gaps & challenges, fundamental rights implications, and funding opportunities[8].

4 Ibid. p10.
5 9622/22, p.17
6 Ibid.
7 See Annex II
8 A sample of the questionnaire is available in the annex of this document.

The questionnaire was distributed, at the Hub members' discretion, to innovation contact points in the MS for further distribution to interested parties.[9] Some agencies felt they could not contribute to this exercise in the absence of an established stakeholder community, while others considered themselves already in the position to reply to the questionnaire on behalf of their respective community based on previous consultations.

For those agencies who circulated the questionnaire to their communities directly, despite several reminders and an extension of the response time to 5-6 weeks, the overall response rate remained low. Moreover, the responses that were submitted varied significantly in quality: some respondents provided extensive, well reflected answers whereas others limited their input to the minimum.

After having collected the replies, the Hub members made a first analysis of the input, based on their extensive knowledge of their respective stakeholder communities. Subsequently, the Hub members provided aggregated data to the Hub Team who analysed it, compiled it and enriched it with further analysis and recommendations. The results and findings of that work were discussed by the Hub Steering Group on 9 November 2022 and are presented in this document for the consideration of COSI. It takes into consideration the Hub's operational and financial model[10] adopted by COSI.

This report does not provide a comprehensive inventory of all innovation actors and projects in the EU internal security field. Instead, it highlights some key projects and implementing actors, and indicates some of the topics considered as important.

[9] For instance, Europol circulated the questionnaire to MS via its European Clearing Board "Tools, Methods and Innovations in the field of technical support of operations and investigations" (EuCB), to the coordinators of the EuCB Core and Strategic Groups, to various EU law enforcement networks and EU research project communities, and consulted with experts in house. All MS were approached through different channels and were given the opportunity to reply.

[10] WK 6558/2021

3. Business needs and gaps

The data collection for this report made a distinction between current and expected future needs. Although there is considerable overlap in the topics identified, the distinction is maintained in the two sub-chapters below.

3.1 Main technological trends

Asked about their main areas of interest, the respondents contributing to the exercise mentioned **AI, encryption and secure communication, drones and biometrics** as the most pressing ones. Given the nature of those topics, many have interdependencies. The topics highlighted by the stakeholder community share many similarities with the Hub's current priorities and ongoing projects, thus confirming the importance and urgency of the subjects in question.

- In the field of **Artificial Intelligence** (**AI**), respondents considered transversal topics of high importance, such as applications of AI in relation to process improvement and resource optimisation, including enhancing automated or semi-automated responses to requests. In the same vein, the transformation of speech into text (including dialects and jargon) is considered a *priority*, along with other use cases based on natural language processing (NLP). Respondents considered it an important challenge to develop systems capable of collecting, collating, refining and classifying information gathered from open sources with the aid of AI. Other topics of interest highlighted by respondents included: protection from 'black-box' AI algorithms; behavioural algorithms based on human factor attributes such as emotion and stylometric analysis; and the creation of collaborative platforms for proprietary or open-source AI algorithms. The respondents also highlighted the importance of public opinion concerning the use of AI in internal security, data and the need to develop trustworthy and explainable AI.

– As for **biometrics**, respondents were interested in robust and secure biometric identity verification processes in order to verify end users' identities in remote digital transactions thereby reducing fraud rates and enhancing confidence in remote digital transactions and contracts. Specifically, Morphing Attack Detection (MAD) solutions (e.g. to help detect passports with *morphed* images) were mentioned, as well as palm biometrics. An Automated Biometric Identification System (ABIS) could improve response times by providing instant results for search requests. Challenges relate to the quality of images capturing different biometric features, fast feature extraction and comparison, and continuous improvement of accuracy, data security, and robustness. Another challenge is the verification of identity using biographical and biometrical identifiers, which might take place in the field but requires connectivity with a database hosted in a secure location (e.g. immigration office, embassy, police station).

– **Facial recognition**, while recognised as a topic within the field of biometrics, was ranked as a topic of high relevance in general. Respondents emphasised their interest in deep learning for use in biometric recognition/identification systems, and for the detection of morphing attacks (including the detection of new attack vectors). The processing of facial images obtained from diverse sources (such as cameras using the red-green-blue (RBG) colour model, thermal cameras and 3D cameras) is considered a challenge.

– Respondents *identified* **Virtual Reality** and **Extended Reality** as relevant topics, e.g. for operational training and the visualisation of cybercrime evidence for investigation purposes.

– **Decryption** of encrypted communication for the purpose of law enforcement investigations remains a topic of high relevance for internal security practitioners. Similarly, actors throughout the internal security sector rely on **secure (encrypted) communication** systems for their own work, and are involved in discussions about the design and adoption of new solutions.

– Respondents recognised *the* importance of tools to support investigations involving **cryptocurrencies**.

– Many emerging technologies, including those mentioned above, will help to shape the development of the future **metaverse**[11], which is consequently high on the operational agenda.

– **Drones** (including nanodrones) will be useful to provide a better overview of crime scenes and thereby increase forensic capabilities. They could potentially increase investigators' safety and minimize the contamination of crime scenes. Such tools need to be tested to better understand both the capabilities and limitations of the systems available on the market.

– Respondents expressed interest in the use of **high altitude pseudo satellites** (**HAPS**), e.g. for their potential surveillance and communication capabilities. The Hub is currently undertaking a study on HAPS funded by Frontex, and thus will be well placed to share knowledge on this matter with the EU internal security community. As well as showing interest in utilising drones and/or HAPS for internal security purposes, respondents also expressed the wish to test the capabilities and limitations of systems to detect and/or disrupt their use by criminals and other actors.

3.2 Future topics

The survey also gathered information about planned projects in the EU Member States. The main areas of interest among the respondents again related to **AI** and **biometrics**.

In the latter case, **biometric** security and morphing attack detection were mentioned, as well as facial recognition on partial or poor quality images, periocular-based identification, and the disentanglement of facial characteristics to allow controlled face synthesis.

There is strong demand for **privacy-enhancing technologies** which could deployed in conjunction with biometric processes and technologies. Respondents wish to explore the further enhancement and maturity of data protection and privacy arrangements, and incorporate such research findings into their future products and services. The Hub is currently undertaking a study on privacy enhancing technologies funded by Frontex, and thus will be well placed to share knowledge on this matter with the EU internal security community.

---

11 https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know

Regarding **AI**, topics considered relevant for the future included anti-spoofing technologies and deep fake detection, both of which could be used to develop effective counter-measures against increasingly sophisticated attack techniques. A known topic, Natural Language Processing (including text to speech/speech to text, especially for dialects and jargon), is expected to remain relevant in the future. The same applies to image and video analysis to increase work efficiency and reduce workloads by automating certain time-consuming tasks (e.g. analysing surveillance camera video material), and the digitisation of crime scenes (including mapping, semantic segmentation and object detection). Chatbots were mentioned, as well as the continuous improvement in speed and accuracy of face, fingerprint and iris recognition technologies. In terms of hardware, demand was expressed for an improved iris image acquisition device. The requirement for explainable AI is expected to remain a matter of concern, and internal security practitioners foresee the need to work proactively on this topic.

A relatively new topic on practitioners' agenda, met with great interest, is **Quantum Computing**. In particular, respondents provided information about ongoing research in Post Quantum Cryptography, i.e. cryptographic algorithms to secure systems against a cryptanalytic attack by a quantum computer.

These priorities partially overlap with a previous collection of innovation topics considered most relevant in the future by the Hub, dating back to 2021. This collection identified AI (including accountability and ethics), biometrics, secure communication solutions, physical security, encryption/decryption technologies, sustainability, development of Open Source Intelligence solutions, virtual reality/augmented reality, novel sensor solutions and technologies for border surveillance and blockchain technology and its applications, ranked in descending order of importance, next to additional domains for future development such as autonomous systems, cyber security, data analysis and visualisation/presentation, forensic and toxicology analysis, disinformation management, quantum computing, satellite imaging, training/education and social research insight. [12]

In sum, the need to anticipate and respond more rapidly to emerging threats is clearly growing. Therefore, further work in identifying and exploiting new opportunities and capabilities, new technologies for research, monitoring, surveillance and responses in digital environment; as well as foresight and anticipatory capacities are being highlighted.

[12] EU Innovation Hub for Internal Security infographic #1213222

4. Challenges

4.1 Data related challenges:

One of the main challenges indicated by the respondents was that their access to datasets for the training of algorithms was limited, or that the datasets available to them were of insufficient quality and/or lacking in diversity. Several respondents underlined that the Covid-19 pandemic had further exacerbated the situation, and data collection processes had been limited or even stopped completely.

According to the responses the lack of appropriate data (clean, homogeneous, operational, structured, in sufficient quantity), especially domain-specific training data (e.g. related to specific crime areas or operational cases), is one of the main factors hindering the building of reliable AI models.

Data science and AI research are data dependent and as such, the first challenge for such research is the data itself. For the last 5 years tremendous progress has been achieved in the field of AI, transforming laborious human analysis and tailor-made algorithm processes into quick and efficient statistical machine learning steps. The accessibility of such tools is an asset that cannot be ignored, but good machine learning (meaning obtaining useful and reliable results) requires good datasets, which must be the basis of any business-oriented automated learning. The "gold standards" (business-oriented and structured relevant datasets) are especially crucial because of the public's high demand for transparency, explainability and reliability whenever AI tools are used for internal security-related purposes.

Building a good quality dataset is a challenge in itself. All research consortia face serious challenges in building sufficiently large and high quality datasets to train algorithms, as operational data is both confidential and sensitive, and subject to restrictions due to low data availability and restrictive legal frameworks. This difficulty is a recurrent theme in projects involving research and technology organisations who are supposed to develop AI tools based on data sets provided by public authorities.

For reasons of acceptability and reliability, AI tools must be trained with the highest level of data quality to be as effective as possible. Building a training dataset requires sufficiently structured, qualified, annotated and homogeneous data, as close as possible to the operational data, and the building of a dual training environment.

Respondents suggested several solutions to this challenge, such as (i) anonymised data, (ii) simulated data or (iii) operational data used within the premises of the participating law enforcement agency (LEA). In light of the requirement to avoid bias, false positives and erroneous results, some parallel difference studies between the three different proposals mentioned above showed that in the first two cases (i) and (ii), links, inferences and correlations, cross-checks and cross-references could be lost, leading to potential misinterpretation and loss of meaning. Proposal (iii), having a training platform within an LEA's premises and having the tool trained by police officers, is rare due to the local lack of knowledge, of availability or authorisation. However, if these conditions can be met, the deep learning with operational real data could lead to more accurate results. The deep learning step is crucial to the future relevance, efficiency and reliability of the tool.

Specific rules apply to operational data, defining the modalities for gathering and sharing data within a research consortium. For example, operational police data are not ruled by the EU General Data Protection Regulation (GDPR) but rather by specific applicable legal provisions (notably the Law Enforcement Directive) that highlight data protection, confidentiality and need-to-know access. The principle of privacy by design and the limited sharing opportunities limit data exchanges within research project consortium, academics and private companies. Opportunities for such exchanges are even more limited when the operational data is classified. Therefore, structuring a relevant dataset, especially with adequate and domain-specific data, is of the utmost importance. This requires the development of appropriate methods to generate high-quality, realistic and representative data, while preserving data protection. This capability, the tools to collect data (unstructured and structured), to clean it and to parse it to reach homogeneity and relevance, has yet to be developed to a sufficient extent, considering the number of projects requiring such data. The larger the dataset is, the more relevant and useful it will be.

The creation of domain-specific learning data is crucial in order to train and test tools. No less crucial is the need to provide training on AI for internal security practitioners and decision makers, in order to avoid misuses and unrealistic expectations, as well as to make research project results closer to the end-users and with a higher technology readiness level (TRL).

The practitioners request a broader standardisation of legal provision within the European Space (EU and associated countries), a core training curriculum for the stakeholders and a collaborative and controlled data training platform. Standardisation should be used to control data quality, and to assess, calibrate and evaluate the performance of the algorithms for higher accuracy.

4.2 Project-related and 'uptake' challenges:

The respondents, as all project practitioners, encountered similar challenges while managing their projects. Lack of availability of knowledgeable staff and limited funding were both mentioned several times, as was the experience of requirements significantly evolving before a project satisfies the end users' needs.

Overall there are many innovative initiatives underway in the MS. However, they are often stopped at the proof of concept (PoC) phase, because of the various difficulties related to getting buy-in, funds and other resources to integrate AI aspects into projects. Respondents also mentioned the challenge of keeping pace with continuous improvements in technologies and to staying up to date with the state of the innovative technologies.

The limited availability of suitable hardware, due to high demand and supply chain problems, is another challenge that innovation projects are facing currently. As a result, combining hardware cost efficiency with the highest quality standards is an associated challenge.

The respondents also underlined the difficulty of finding customers willing to adopt or trial solutions at an early stage. Very often the challenge to face is how to ensure and support the continued development of solutions in the absence of a customer.

Very often, fragmented/decentralised procurement and research and innovation initiatives, as well as a lack of information sharing and knowledge management, hinder opportunities and broader efforts towards innovation within the national authorities.

Respondents also highlighted the very limited human resources allocated to R&I activities, and the lack of knowledge of relevant technological capabilities, among operational stakeholders.

This topic will be covered in more depth in an upcoming Commission report on Security Research Uptake.

4.3 Training and knowledge related challenges:

The respondents mentioned the lack of knowledge about new technologies from decision-makers and stakeholders as one of the biggest challenges they face. This lack of knowledge can lead to unrealistic expectations from AI systems, which in turn can result in disappointments and/or misuse.

However, the same lack of knowledge can also result in the opposite trend, namely resistance to change, unfounded mistrust of new methods and tools and strong preferences for old technologies and legacy systems.

4.4 Legislative and regulatory challenges:

The majority of respondents mentioned challenges related to the legal and regulatory aspects of their work.

The lack of a clear legal framework dealing with access to data within research and innovation projects, and/or the lack of stability therein (e.g. due to the ongoing work on the EU AI Act) was identified as a main factor hampering AI and other innovation projects. The absence of a clear and well understood regulatory model for AI, and innovation more broadly, means that the national authorities, academia, research and technology organisations and local project practitioners face a lack of harmonisation in the requirements of their customers and partners. They also face a reluctance to invest in the innovation, due to the unclear future regulatory environment. The Accountability Principles for AI Project (AP4AI) is one of the five pilot projects coordinated by the EU Innovation Hub for Internal Security. It seeks to provide a framework and roadmap to guide internal security practitioners through the planning, development and deployment of AI tools in full compliance with accountability principles and EU values while anticipating all possible regulatory requirements.

5. Fundamental rights implications

The questionnaire sent to the Hub's stakeholder community included a section on fundamental rights implications. One question asked the respondents to identify the fundamental rights they considered most relevant in relation to projects using innovative technologies.

A clear majority of the respondents stressed both privacy and data protection as having the greatest relevance. It was however worth noting that most respondents listed several rights in great detail, The most frequently mentioned ones include human dignity, non-discrimination, freedom of expression and information, right to effective remedy and to a fair trial, right to physical and mental integrity of a person, freedom of assembly and association, equality before the law, prohibition of torture, inhuman or degrading treatment or punishment, presumption of innocence and right of defence, as well as rights of the child.

In response to the question as to whether stakeholders with fundamental rights expertise had been involved in their respective projects, a huge number of respondents and directly involved fundamental rights actors. Among those mentioned, the European Data Protection Supervisor (EDPS), the EU Fundamental Rights Agency (FRA) and the Council of Europe (CoE) featured most prominently among the institutions/actors, as well as more generally civil society, ethics advisors, national human rights institutions, equality bodies, internal oversight mechanisms, and universities as advisors.

In terms of measures taken to protect fundamental rights, respondents declared and illustrated an elevated awareness level of the legal instruments available in the EU, including the EU Charter of Fundamental Rights, GDPR, and the incoming EU AI Act. The Code of Conduct for Research Integrity established by Horizon Europe Regulation 2021/695 was also mentioned.

Respondents described fundamental rights assessments, integrated in all process steps, and built into the project methodology. They also reported comprehensive and continuously updated vulnerability assessments, risk assessments and threat assessments. Due to the high level of awareness, information sharing, evaluation, and cooperation with those affected, as well as involving subject matter experts during the entire project lifecycle, strong independent oversight and effective remedies could also minimise any risk of potential negative impact on fundamental rights. The respondents also considered the social acceptance of tools and the importance of proportionality, and quoted established concepts such as referred to data protection by design and default, ensuring the chain of custody in e-evidence, and audits, in their replies.

Specifically in the field of AI, respondents highlighted as fundamental rights safeguards the requirement for a legal basis for the processing of data and the need to justify a legitimate interest. They also mentioned data minimisation, logging of activities (centralized logging and data access management) and transparency, for the "human in the loop", rigorous testing for bias, diverse data sets, and the avoidance of any unfair representation of segments of the population.

6. Funding instruments

The majority of respondents to the questionnaire use EU funding, in particular the EU Internal Security Fund and Horizon Europe, as well as Digital Europe and Horizon 2020 to a lesser extent.

National funding plays an important role as well, but is mostly combined with EU funding instruments. This is not surprising since ISF and some other funds require such "co-financing".

sA small but remarkable number of project leaders carry out their work without relying on any funding instrument.

Respondents expressed interest in cooperation opportunities with other (funded) projects, in particular for the identification of new use cases, acquisition of training and test data, and pilot installations (including user-feedback).

7. Technology trend monitoring

The questionnaire included a section designed to understand better how the internal security communities monitor recent trends in technologies and ensure that they remain up-to-date. On the basis of the feedback provided, it can be said that the main sources of information about technology trends are being a member of research communities, interacting with the scientific community and active discussions with partners (industry, academia) and customers. Participation in international conferences, workshops, meetings with technology providers, testing activities within research projects, trials, demonstrations and trade fairs on innovation related topics and technologies (e.g. AI) were mentioned by most of the respondents.

The respondents also regularly review the academic research literature, analyse the trends on the market, review media coverage and monitor funding programmes.

Additionally, the respondents conduct their own studies on new and emerging technologies, and perform technology foresight exercises with the support of the relevant experts.

8. Cooperation with the EU Innovation Hub for Internal Security

The survey sought to gather information about perceptions and expectations of the EU Innovation Hub for Internal Security among the MS Authorities, practitioners, research and technology organisations and academia. Respondents would like the Hub to support the initiation of new projects and to help identify funding opportunities and partners. The vast majority would also like the Hub to share expertise and knowledge. They would welcome the opportunity to participate in events organised by the Hub. Respondents would like the Hub to get involved in existing projects, especially for promotional and dissemination purposes. Last but not least, the cooperation with the Hub was also seen as offering added value in the distribution of results and the standardisation of project outcomes.

9. Conclusions and recommendations

Based on the input received from the MS innovation community and the EU Agencies' and their stakeholders' contributions, the Hub mapping exercise generated the following conclusions as well as some recommendations how to implement them.

9.1 Data collection for the mapping exercise:

Based on the experience of the approach described in chapter 2 above, the Hub considers that a questionnaire might not be the only instrument to collect such information, considering the high investment compared to the low response rate, and taking into account the varying approaches of Hub members. The main strengths of this approach were to achieve outreach to the wider stakeholder communities in the MS and to establish a qualitative overview.

Recommendation 1:

Similar exercises in the future should be designed in a more targeted way in order to access available knowledge, analyse it and provide recommendations. For example, research methods such as focus groups and semi-structured interviews could be considered. As soon as the Hub is better known in the MS and has increased its visibility, the Hub expects better results by reaching out to its stakeholder communities using a varied approach.

Action for the Hub:

Continue to regularly collect knowledge/information on innovation initiatives, by making use of a wider range of methods.

Continue to promote the Hub including its mandate and mission, among its stakeholders in the Internal Security area.

9.2 Information sharing platform:

Most innovation-related projects in the EU focus on developing new technologies. Many of them seem to operate in isolation, not necessarily aware of similar solutions being developed in other countries. They often lack information about the outcomes of other relevant projects that could allow them to build upon existing findings from predecessors instead of starting from scratch.

The vast majority of projects and solutions that MS are developing are intended to be scalable, and most of the project leaders are interested in cooperation with other MS/ practitioners in order to create synergies. Therefore, a platform listing both projects and contact details would be very helpful for MS when identifying potential partners and customers.

Recommendation 2:

A platform to exchange information and promote new projects and solutions would be most beneficial for MS when searching for partners, customers, and expertise. The Hub could be instrumental in being/providing such a platform, in line with its base task of knowledge management and providing a common innovation picture for internal security.

Action for the Hub:

Explore existing solutions, consider options, and further define the requirements, for a platform to collect/share information on ongoing projects/pilots, open to MS, that would serve as a catalyst for synergies or initiation of new projects. The implementation of such platform however is scalable. Its feasibility and scale need to be further assessed and, depending on the availability of funding and resources, be included in the Hub's multi-annual planning proposal.

9.3 Data:

The respondents identified easier access to data (including data for training and testing algorithms) and a clear data sharing policy as crucial requirements for meaningful data acquisition and to strike a balance between internal security efficiency and fundamental rights. Necessities include better model training, and reliable testing results and innovation progress.

Respondents have also identified a need for clear and well-defined legislation in the field of innovation, in particular concerning the use of AI and the use of data for AI.

Recommendation 3:

The European Commission is currently exploring the possibility to develop a European Data Space for Innovation in the field of internal security. In addition, all Agencies contribute to the topic. Europol was given a legal basis to use operational and personal data to develop, train and validate AI models to support police work with the support of its permanent law enforcement AI expert group. eu-LISA is operating a Working Group on AI with its MS; and Frontex' has extensive operational and statistical datasets and experience in data processing and management. These initiatives could address a number of the requirements mentioned by MS practitioners and EU stakeholders alike. A strong role of the Hub in the development and running of such initiatives would ensure that operational needs are met and fully serve their purpose and are in line with fundamental rights standards.

Action for the Hub:

Support the development and promote the use of the European Data Space for innovation by the internal security community.

9.4 Funding:

The respondents mentioned additional funding at EU level for the development and implementation of innovation projects as important for the further work on innovative projects.

Recommendation 4:

Whereas the increase of funding is outside the Hub's remit, it could contribute to a more efficient use of existing resources. Several of the JHA agencies represented in the Hub already have a role in the Commission's establishment of calls, and the evaluation of project proposals (in the framework of the EU's Research and Innovation funding programme). The Hub, with its cross-sectorial outreach to relevant EU internal security stakeholders will be instrumental to contributing to the entire lifecycle of EU project funding to support innovation in the internal security domain, from identifying topics for the launching of calls to the uptake of finalised project results, and to ensure a user-friendly environment for innovators in the internal security sector. Such a role would, however, only come into effect if and when the role of the Hub goes beyond the contribution of individual agencies and should not duplicate that, e.g. through the Hub identifying new areas of research through its cross-sectorial helicopter view on innovation in the internal security sector.

Action for the Hub:

Contribute to a more efficient use of existing resources at EU level, in particular by contributing to the identification of relevant topics for the EU Research and Innovation funding programmes, and the uptake of the finalised projects results. The actual Hub contribution would have to be detailed in its multi-annual planning.

9.5 Role of the EU Innovation Hub for Internal Security

As to the role of the Hub, the respondents imagine a platform to facilitate engagement between potential partners, e.g. as early adopters of technology, or as a place to showcase new technology solutions, whether developed by Hub members, national authorities, research and technology organisations or others. Key innovation actors see the Hub's future as a knowledge repository which promotes knowledge sharing and provides "organisational memory" for knowledge and results achieved by temporary projects, as well as communication between MS. The Hub is expected to create synergies by providing a platform and shared channel for all such actors.

The Hub is understood to be the place where trends are monitored, and assessments shared with the internal security community, with a view to supporting MS in their decision-making as to which trends and projects are worth investing in.

Recommendation 5:

As per recommendation 1, relying on the sectorial knowledge of the Hub members, the Hub could fulfil such role as central knowledge repository and platform for exchange. It can further support and promote cooperation between the foresight capabilities and different expertise of individual Hub members for the benefit of the MS. The Hub can also provide a platform to explore and test novel ideas and innovative approaches relevant for different sectors of the internal security domain, including vis-à-vis their fundamental rights compliance. Informed by the knowledge gained through such engagement with MS, and its own mandated activities, the Hub would be in a position to contribute to policy discussions at EU level on innovation matters.

The Hub is well placed to support EU MS in their innovation activities as described above, provided there is the necessary engagement by MS, and sufficient commitment from the Hub members and EU institutional actors to turn the Hub into a sustainable and effective instrument to increase the positive impact of cross-sectorial innovation activities in internal security.

Action for the Hub:

Act as a central knowledge repository and platform for exchanges, to explore and test novel ideas and innovative approaches across the internal security domain, to support MS, and to contribute to policy discussions at EU level on innovation matters.

Recommendation 6:

Strengthening the Hub, through more consistent engagement from its members and greater visibility for Member States, is therefore an underlying recommendation as to facilitate the tasks outlined above and which were assigned to the Hub by COSI.

10. Next steps

The Hub Steering Group endorsed the present report on 9 November 2022 and agreed to present it to the COSI. It should then form the basis for a multiannual plan for the Hub's work, as previously defined by COSI, covering four years to be reviewed every two years and with the possibility to adapt the prioritisation in case of extraordinary events. Such a multi-annual plan will be provided to COSI, after approval by the Hub SG, at a COSI meeting in the first semester of 2023.

In addition, this report should serve as a useful source of information for the Member States (via COSI) and the European Commission, for the further development of its internal security research and innovation agenda.

Annex I:

Online questionnaire uploaded in EU survey (model version used by Europol): **EU Innovation Hub for Internal Security - Mapping of innovation actors and projects**

Annex II:

The questionnaire was distributed by the Hub members to their respective communities of experts and stakeholders. Taking into consideration the diversity of each Hub member's operating field, the provided answers provided snapshot of innovation trends, needs and challenges in the various areas within the internal security domain.

The contacted communities consisted usually of appointed delegates from MS, other government institutions, academia, and small-to-medium enterprises (SMEs).

Frontex replied to the questionnaire on behalf of their respective community, based on previous consultations. Some of the Hub Members felt they could not contribute to this part of the exercise, in the absence of an established stakeholder community.

List of main stakeholders and stakeholder groups to whom the questionnaire was sent:

- 27 Member States law enforcement competent authorities and Ministries of Interior
- Europol Innovation Lab and EU Clearing Board for Innovation (EuCB)'s core groups and strategic groups (specifically AI, ethics and foresight).
- Community for European Research and Innovation for Security (CERIS)
- Research and Technology Organisations (RTOs) and universities participating in EU-funded R&I projects
- EARTO (European Association of Research and Technology)
- ENFSI (European Network of Forensic Science Institutes)
- ECTEG (European Cybercrime Training and Education Group)
- ILEA-net (Innovation by Law Enforcement Agencies networking)
- I-LEAD (Innovation - Law Enforcement Agencies Dialogue)

- ENLETS (European Network of Law Enforcement Technology Services)
- EACTDA (European Anti-Cybercrime Technology Development Association)
- European Association for Biometrics
- Selected Europol operational experts
- 8 innovation projects, 15 civil society organisations and 10 individual experts, selected upon advice of the experts of the EU Fundamental Rights Agency (FRA)
- CEPOL National Units
- EMCDDA Scientific Committee
- EMCDDA Reference Group on drug supply
- EUAA Asylum Processes Network
- eu-LISA Security Officers Network (SON)
- eu-LISA Working Group on AI
- eu-LISA Biometric Working Group
- Virtual Community Joint EU forces on AI – network led by EFSA