Council of the European Union

Brussels, 19 February 2020
(OR. en)

6158/20

LIMITE

CT 10
COSI 25
CATS 14
ENFOPOL 46
JAI 130
TELECOM 18
CYBER 21
RECH 44
CFSP/PESC 145
CSDP/PSDC 87
HYBRID 3
RELEX 135
ESPACE 7
IND 22

NOTE

From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	Embracing new and disruptive technologies in internal security and justice with an EU Innovation Hub

In October 2019, the JHA Council endorsed[1] a proposal by the EU CTC to establish a European multi-stakeholder entity for **innovation in internal security and justice**[2].

1 The JHA Council of 8 October 2019 (Doc. 12837/19): "*Ministers expressed their overall support for the creation of an innovation lab at Europol which could act as an observatory of new technological developments and drive innovation, including by developing common technological solutions for member states in the field of internal security.*"

2 Disruptive technologies and internal security and justice of 8 May 2019 (Doc. 9069/19). The proposal is a joint product of a seminar gathering 40 senior EU executives from European institutions, agencies and MS.

This joint structure would be an **EU Innovation Hub** ("The Hub")[3], a common platform to support and deliver products and services, by capitalizing on respective expertise of European security actors (i.e. the research and innovation entities from European Union (EU) agencies such as the Frontex R&I Unit or the planned Europol Innovation Lab[4]), to initiate common pilot projects; boost opportunities and mitigate the substantial risks and threats associated with new technologies; maximize the utility of data; de-conflict legal challenges tied to operational needs; and anticipate the necessary transformations of mind-set and organisations.

By jointly achieving the above, the Hub would help to **collectively and concretely address the rising and fast-evolving challenges faced by all Members States (MS) and European agencies** owing to emerging technologies. Beyond, this Hub would contribute to and advance the EU's position as a global leader in disruptive technologies in the field of internal security and constitute an urgently needed step towards increasing **European technological sovereignty**[5]. In doing so, the Hub will help reduce the EU's technological lag vis-à-vis its global strategic rivals moving at far higher speeds (mainly China and the United States).

This note is meant as a contribution to the ongoing work led by Europol focusing on the tasks of the Hub. The agreed upon tasks should drive the discussions on governance and means for its implementation. It will be necessary to urgently provide adequate funding for the Hub distinct from the equally necessary funding of a Europol Innovation Lab. It's crucial to keep a high level of ambition in order to pave the way to an advanced EU capacity catalysing innovation and delivering cutting-edge products for the security of European citizens.

---

3 While initially called the "joint innovation lab for European agencies (the "lab"), it has since been renamed the "EU Innovation Hub" to avoid confusion with innovation labs of EU agencies and to better describe its role.

4 The Deep Dive of 17 July 2019 led by Commissioner King on emerging technology, security and law enforcement supported a joint venture between Europol and JRC "*to start the work immediately*". Such a tool focused on law enforcement would be a sound building block for the EU Innovation Hub's activities.

5 See "A new strategic agenda 2019-2024" agreed by the European Council in June 2019; "The Political Guidelines for the Next Commission 2019-2024" of July 2019.

I. A multi-stakeholder Innovation Hub

The EU Innovation Hub ("The Hub") would bring together relevant EU and Member States security and justice **stakeholders**, gathering agencies of Member States, EU JHA agencies (Europol, Frontex, Eu-LISA, Cepol and Eurojust), other EU institutional actors and agencies playing a role in security (Joint Research Centre [JRC], Enisa and the European Monitoring Centre for Drugs and Drug Addiction [EMCDDA]), military and space (European Defence Agency [EDA], EU Satellite Centre [SATCEN], European Space Agency [ESA] and European Global Navigation Satellite System Agency [GSA]), the EU Institute for Security Studies (EUISS), the European Data Protection Supervisor (EDPS) and the Fundamental Rights Agency (FRA), the European Investment Bank (EIB), practitioner networks such as the Expert Group on the Use of AI for Security set up by DG HOME, ENLETS[6], SEREN4[7], I-LEAD or ILEAnet[8], the relevant European security, military and space industries, and European academia and private sector more broadly (from start-ups, through small enterprises to large corporations, including venture capital firms), across the entire value chain (research and development, investment, production), with a view to enhancing the EU's technological prowess and developing products intended for industrialization from the get-go.

The Hub will **build on but not replace the existing structures** thereby bringing together diverse and most advanced expertise within the EU to develop cutting-edge initiatives. Hence, it will connect Members States' and EU innovation capacities active in internal security and justice.

---

6 The European Network of Law Enforcement Technology Services (ENLETS) started in 2008, to operationally strengthen police forces and to promote the use and development of technology by exchanging information, experience and knowledge on a practical communication level.

7 SEREN4 is the security research network of national contact points for Secure Societies Challenge in Horizon 2020 (H2020 SC7); funded by H2020, it offers direct assistance and opportunities to practitioners for learning, training and networking, creating synergies with key security players in the field of security research.

8 ILEAnet is the European LEA Research and Innovation Network, started in 2017 and gathering 19 partners from 16 European countries, to support LEAs in the domain of security research.

According to the JHA Council of 8 October 2019, the Hub will be headquartered at Europol. This will allow it to take advantage of technological expertise developed by Europol[9], and the potential offered by joint work on technologies with Eurojust as well as the connection to a wider ecosystem[10]. This location would also ease the direct connection to policy-making level in Brussels.

The Hub could be created by an administrative agreement between EU agencies[11]. It is crucial to give the Hub sufficient **resources** for adequate staffing and for funding its own pilot projects, in addition to the possibility of grants from EU-funded research programmes. It would rely partly on experts seconded by the stakeholders.

The structure and governance model should be kept **inclusive, agile and dynamic**. The main governance body should be composed of EU agencies. Other stakeholders would be invited to join the activities of the Hub, on a voluntary basis, according to a task force model, to address common challenges or implement projects where underlying technologies are similar. The Hub might operate in a decentralized manner by placing one specific stakeholder in charge of an activity who will aggregate relevant work streams (e.g. give JRC the lead on a specific law enforcement project such as vehicle forensics, together with European industrial partner(s) and Member States' entities). For all its tasks, the Hub must leverage creative research and innovation methods, embrace risk taking, give researchers the freedom to fail, and launch projects measured in weeks or months rather than years or decades. The choice of individuals who embody these values is paramount. It will help break silos in the security and justice community across the EU.

---

9 Building on its expertise in the field of technologies (encryption, cryptocurrencies, fight against terrorist content online, etc.), the Europol Strategy 2020+, adopted in December 2018, identified innovation and research excellency as the 4th strategic priority. Europol produced a report on "Exploring Tomorrow's Organised Crime" in 2015 and a second one on "How technology shapes the future of crime and law enforcement" in 2019.

10 United Nations Interregional Crime and Justice Research Institute (UNICRI) has headquartered its Centre for AI and Robotics in the Hague, which has partnered with INTERPOL's Innovation Centre. NATO Communications and Information Agency (NCI) is partially based in The Hague.

11 The inter-institutional agreement creating the CERT-EU, an *ad hoc* structure working in network with Member States' CERT entities, could serve as an example of a top-end tool.

II. Driving Research and Innovation in technologies for internal security

The EU Innovation Hub (the "Hub") would have five primary tasks: **i) initiating joint pilot projects in accordance with a 'DARPA'-type methodology; ii) evaluating the risks and opportunities presented by new technologies; iii) optimizing data use for operational needs; iv) de-conflicting laws with operational requirements;** and **v) reflecting on necessary personnel and methodology transformations**.

1. Initiating Joint Pilot Projects

The Hub would **initiate joint pilot projects** to develop practical products based on emerging technologies to respond to operational users' needs while fostering the European security-industrial basis. Projects would ease technical interoperability across EU and MS security and justice actors. Projects should aim for industrialisation from the outset, through the close involvement of, and cooperation with the European private sector, thus facilitating market uptake.

Vital to the success of the Hub and its pilot projects, is the employment of a **'DARPA' methodology**[12], which affords the flexibility necessary for (potentially, iterative) scientific experimentation. Specifically, it will be necessary to be able to quickly release sufficient capital with the freedom to fail and encourage tests and prototyping, all with a light, flexible and autonomous decision-making process, flat hierarchy, as well as a rapid turnover of personnel throughout the structure, short-cycle and light assessment reports, and rapid judgment on whether to accelerate or give up. The choice of the managers will be key in achieving this.

According to the DARPA methodology, the Hub would need its own discretionary budget devoted to funding its pilot projects, in a rapid and flexible manner. In parallel, the Hub would explore the best use of the different research and innovation (R&I)[13] funding sources available under the current and next Multi-Annual Financial Frameworks (MFF), if appropriate[14].

---

12 The US Defence Advanced Research Projects Agency's methodology has resulted in major industrial and technological achievements in both the civilian and military spheres. The proposal put forward by the President of the French Republic in September 2017 for a European research and development agency for disruptive technologies, along the lines of DARPA, merits consideration and implementation.

13 See COM(2018) 306 final of 15.5.2018 "A renewed European Agenda for Research and Innovation - Europe's chance to shape its future".

14 Digital Europe, COSME, Internal Security Fund; Horizon Europe, InvestEU or the European Defence Fund.

In addition, the Hub could advise stakeholders on the availability, eligibility and access method to the wide range of existing EU funding sources under the current and next MFF[15]. The Hub could act as a catalyser for stakeholders by suggesting the creation of consortia or informing them of existing consortia applying for EU-funded projects. Beyond, the Hub could initiate a reflection with its stakeholders (mainly the EBI and the financial private sector), on the design of new funding instruments, and experiment with their implementation.

The Hub could develop **projects from short term to longer term**, based on existing projects in the EU and identification of future opportunities (e.g. admissibility of e-evidence, predictive police, automated translation and natural language processing, voice analysis and object recognition, etc.). In the short term, the Hub would support the mutualizing of current projects[16], and launch technological projects covering unaddressed tactical needs (e.g. the use of blockchain for exchange of information by Eurojust Joint Investigation Teams). The Hub could also spearhead work on the next waves of disruptive technologies (post deep-learning techniques in AI, 6G, etc.). Pilot projects will also embed ethical considerations at their inception to ensure their sustainability.

The Hub would **disseminate the concrete results** of both its pilot projects and results of interesting security research and innovation projects across its stakeholders. The Hub could create a dashboard allowing easy access to on-going and completed R&I projects at both EU and MS level. Furthermore, the Hub could make available best practices with regards to procurement rules for innovation[17], or could be invited to develop new practices[18].

---

15 The Hub could create an online tool for EU funding and EBI lending, akin to IdentiFunding developed by the EDA and learn from Member States' experience, such as the Spanish Security Technological Centre (CETSE) at the Ministry of Interior in charge of *inter alia*, maximizing synergies between EU funding instruments.

16 Frontex organises demonstrations of technology, conducts technical feasibility studies and runs pilot projects for borders, to test potential solutions and assess their capabilities as well as identify future needs.

17 *Inter alia* the EU Directive relating to defence and security procurement; Pre-commercial Procurement for innovation (PCP) or Public Procurement of Innovative Solutions (PPI).

18 Based on the Commission's work in this field such as the 'Innovation Public Procurement Guidelines' or its recommendation to explore joint innovation procurement for AI in its communications on AI published in 2018.

2. Assessing Risks, Threats and Opportunities and Horizon-scanning

The Hub would lead two parallel assessment activities.

2.1. First, it will **assess risks, threats and opportunities** posed by emerging technologies or novel applications of existing technologies. On this basis, it would suggest mitigation measures or ways to exploit opportunities created by the on-going and ever-accelerating technological transformation, including by recommending in-house pilot projects funded by the Hub's discretionary budget[19]. To most effectively achieve this task, the Hub could partner with European structures[20] or with academia[21].

Its products are intended to **alert and inform policy makers** (e.g. the need to engage with the international working groups shaping standards to ensure that requirements preserving the capacity of targeted lawful interception are included), feed initiatives (e.g. create capacities to mitigate the use of new technologies by terrorist groups), provide ideas for pilot projects and serve to raise awareness of the risks among the different communities of innovators (e.g. open spaces for biotech experimentation).

They could also contribute to the **identification of industrial-technological priorities** for the EU (e.g. support EU companies developing quantum-resistant cryptography software) and policy initiatives to be taken at EU level (e.g. engaging with tech companies which decided to generalise the encryption of internet protocols by themselves, thus compromising the ability to lawful intercept communications).

---

19 For example. how to mitigate the risk of facing a terrorist attack via miniaturized drones to disperse a home-made bio-bomb over a public space.

20 For example INTCEN (SIAC) as well as agencies (e.g. Enisa produces regular reports on cybersecurity and new technologies like cybersecurity and distributed ledger in 2016, etc.).

21 The Lab would partner with European institutions equivalent to organisations such as The International Risk Governance Centre at Ecole Polytechnique Fédérale de Lausanne (EPFL) or the Royal United Services Institute (RUSI) which has developed a Global Research Network on Terrorism and Technology.

2.2. In parallel, taking inspiration from and in partnership with the space and defence sectors[22], the Hub would engage in **horizon-scanning of the technical, regulatory, institutional, and human capital transformations due to new technologies**, to issue strategic-level recommendations for the EU, based on credible scenarios[23]. This foresight activity would encompass the following elements: i) identify the impact of geopolitical and socioeconomic trends on technologies (e.g. the fragmentation of Internet; how ethical considerations could drive their development); and ii) understand how new technologies and their convergence could impact societies and business in the context of security and justice (e.g. the development of open online labs for genome manipulation). Their aim is to anticipate the impact of both trends on the way we deliver security and justice in the EU (e.g. how to respond to the privatisation of security by tech companies)[24].

This activity could build on existing efforts[25] in this field and could be closely developed with the European Commission Vice-President in charge of Foresight and Institutional Affairs, in order to contribute to the EU decision-making.

3. Optimizing data for operational needs

Given the prevalence of data in so many technology-related fields, the Hub would **create a data lake, promote data integrity** (circumvent bias and counter deep fakes), **and undertake data research** (data-lean AI, next Big Data for criminal analysis, etc.) to transform data into reliable operational outputs.

---

22 The Hub could inspire itself from the EUISS or the French Ministry of Defence Red Team. In the US, the Army has set up a Mad Scientist Laboratory, and the CIA developed a Red Cell after the 9/11 attacks, which seeks to continuously challenge key assumptions, conduct alternative analysis and prepare for US for so-called 'black swan' events (unforeseen, very high impact events like the sudden rise of IS Caliphate).

23 The EUISS published "Scanning the horizon: 12 scenarios for 2021" in January 2019. Another example of crossing of expertise and data among defence, security and space sectors is the report "Implications of Climate Change for the U.S. Army", published by the US Army War College in October 2019 which analyses the impact of climate change on US national security by 2050.

24 Analytical foresight methods, such as 'what-if's', horizon scanning, and scenario-building with design fiction methodology should ensure that the Hub, and therefore the EU, is consistently ahead of the curve.

25 Frontex is currently developing a partnership with the EDA on foresight. Within the Council of the EU, meetings of the Horizon Scanning Network are organized.

In particular, the Hub would analyse how a shared **data lake** could be created together with the support of entities in charge of privacy and data protection (EDPS and European Data Protection Board, FRA, DG JUST, etc.) within the existing legal framework. This data lake would seek to truly pool disparate data in a single entity for analytics as well as training artificial intelligence tools (e.g. to test the potential for detecting radicalisation tipping-points). Such infrastructure, coupled with an ability to deal with data of various origins, would bring real added value to the development of software tools. It would need preliminary work[26] as well as sufficient budget.

4. De-conflicting legal challenges in operational cases

Since security, privacy, data protection, safety and transparency of algorithms may be conflicting norms, the Hub could offer **a de-confliction mechanism for dealing with operational cases**. Concretely, the Hub could offer practitioners and scientists the opportunity to work together with actors such as DG JUST, the EDPS or FRA in order to develop legal solutions to operational requirements which might conflict with existing legislation[27]. The Hub would nurture creative solutions within the existing legal framework as well as reflect on possible changes.

Thus, the Hub could develop both principles and technological tools with the data protection authorities, researchers and internet companies, with the aim of **exploring technological solutions** supporting privacy by design such as pseudonymisation technologies for data transfers, anonymization technologies for data retention, the use of open source or synthetic data, and the potential of differential privacy. The Hub could support the production of specific guidelines for the internal security sector or explore how "regulatory sandboxes"[28] could work in practice to facilitate testing and experimentation of new businesses models not yet regulated.

---

26 The Hub could exploit the work initiated by DG HOME on the topic.

27 E.g. access by LEAs to WHOIS, handling of FIU.net by Europol, reliability of evidence put in question by new technologies, role of chain of custody and cross-examination, etc.

28 See COM(2018) 237 final of 25.4.2018 AI Intelligence for Europe, "*These are testing grounds for new business models that are not (yet) regulated*".

5. Fostering Human Capital

Rapid advances in emerging technologies are changing the very nature of jobs - and the skills needed to do them - faster than ever before. The Hub would therefore suggest the necessary medium- to long-term transformations within security and justice areas, in order to more effectively **detect**, **attract, recruit**, **manage and train, as well as retain talent**. The Hub could act as a testing ground for these innovative practices.

In the short term, the Hub would help identify the profiles needed to **fill impending knowledge and functionality gaps** (e.g. hiring an expert in blockchain, data analysis, algorithm creation and control, data infrastructure management or data labelling) It would also reflect on the medium to long term impact of new technologies on security and justice professions, and advise on the need to diversify recruitment accordingly.

Together with Cepol, the Hub will help develop new and innovative **training** methodologies (e.g. on open source intelligence, facial recognition, etc.) as well as practical training on technological tools (e.g. neutralizing a drone), to be delivered by Cepol for law enforcement, and the European Judicial Training Network for justice area or Frontex for border security. Insights on innovation should include the broad range of actors security and justice, such as staff in charge of public procurement. Student programmes such as those existing in the US should be developed[29].

This could also involve developing new methods of cooperation between academic talent or the private sector and the security professions, which are themselves expected to evolve. Thus, the Lab could collect, develop and disseminate innovate practices on how to effectively **incentivise European researchers to work for security and justice** (e.g. allow them to benefit from patents, offer career progression and benefits on-par with the private sector, the Hub could help connect researchers with venture capital, etc.). Attracting the necessary talent will involve offering opportunities which combine issues of public interest with access to exclusive data or technologies.

[29] Many federal Agencies in the security and space sectors offer opportunities for students (internship, fellowship, scholarship, etc.). The NSA offers various paid programs for high school, college and graduate students in its focus areas (e.g. computer science, language skills in Chinese, Russian, Korean, Farsi or Arabic).

III. Action Recommendations

In the **immediate term**, it is vital that decisions be taken urgently on:

1. Appointment of the Head of the Hub or a "préfigurateur", to ensure clear leadership
2. Agreement on the tasks, to drive the discussions on governance and resources
3. Allocation of appropriate resources, to start as soon as possible
4. Setting up of the administrative governance structure with key stakeholders.

In the **medium-term**, it is key to the operational stability, morale and success of the Hub, that additional resources within the next Multi-Annual Financial Framework are earmarked for it, alongside other financing from sources such as the Internal Security Fund, alternative research-related funding or Digital Europe. Throughout both stages, our ambition should remain high as we pursue the development of a new mind-set and new capacities vis-à-vis emerging and disruptive technologies in internal security.