Council of the European Union

Brussels, 8 July 2020
(OR. en)

9185/20

LIMITE

CT 49	COMPET 294
JAI 538	IND 85
COSI 109	RECH 244
CATS 46	DATAPROTECT 59
DIGIT 51	ENFOPOL 159
CYBER 106	ESPACE 26
HYBRID 15	POLMIL 81
TELECOM 100	SE 6

NOTE

From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	Contribution of the EU CTC regarding the Commission communications of 19 February 2020 on digital, data and artificial intelligence Proposals on internal security and criminal justice

The Commission has set out an ambitious plan to place the European Union at the forefront of the digital revolution[1] in its communications on Europe's digital future[2], artificial intelligence (AI)[3] and data[4]. **Though identified as one of the drivers of this revolution, internal security and criminal justice[5] are still being treated as a poor relative in the European digital model**, since they are not included in the criteria for choosing technology (which prioritise market driven approaches[6]) and are viewed more as risk factors with respect to fundamental rights and personal data.

1 'Digitalisation' denotes a transformation achieved through the use of digital technologies.
2 COM(2020) 67 final, 19 February 2020, *Shaping Europe's digital future* (hereafter: 'digital strategy').
3 COM(2020) 65 final, 19 February 2020, *White Paper on Artificial Intelligence - A European approach to excellence and trust* (hereafter: 'White Paper').
4 COM(2020) 66 final, 19 February 2020, *A European strategy for data* (hereafter: 'data strategy').
5 For convenience, **this note will use the term 'internal security' to cover criminal justice and the term 'criminal' to also include terrorism.**
6 As the 5G affair has shown, security questions are usually raised very late in the discussions, even though these choices may reduce our ability to ensure protection and justice for citizens.

The data-driven economy and disruptive technologies create benefits but also generate new risks from criminal and terrorist organisations, whilst stimulating profound change and worldwide strategic and industrial competition in which the non-European digital giants wield increasing power[7]. Given the very rapid development of these major challenges it is vital, **whilst maintaining strong instruments for protecting rights and freedoms**, firstly to **develop the European digital and data industries in the field of internal security, so as to improve the functioning of security and justice whilst supporting the EU's technological sovereignty and leadership[8],** and secondly to **minimise the risks of misuse and of impunity for criminals and terrorists.**

Whilst the potential for using digital data and technologies to combat serious crime is recognised, **the EU needs a much more ambitious commitment and an appropriate framework:**

- though the White Paper considers it necessary to equip law enforcement authorities with AI tools in order to protect European citizens better against criminal acts and terrorism[9], it views these applications **only in terms of their 'high risk'[10]**. So while references are made to relevant areas for their use, facial recognition and predictive policing are used more to illustrate risks of bias and discrimination[11];

---

7 See EU CTC Note 9069/19 of 8 May 2019 on *Disruptive technologies and internal security and justice*.

8 The term 'technological sovereignty' is used in the data and digital strategies. The industrial strategy uses expressions such as 'Europe's sovereignty', 'strategic autonomy', 'strategic sovereignty', 'technological sovereignty' and 'digital sovereignty'. The notion of sovereignty is to be understood as fostering own European digital and industrial capacities while remaining open to external innovation and technologies under fair market environment; it will allow to build these capacities and competences, in the EU while avoiding creating "European bias". Such a "European bias" would also be avoided by creating data partnerships with selected partners, such as Africa.

9 White Paper, footnote 5: '*identify online terrorist propaganda, discover suspicious transactions in the sales of dangerous products, identify dangerous hidden objects or illicit substances or products, offer assistance to citizens in emergencies and help guide first responders*'.

10 In accordance with the Commission's definition, internal security activities will be classified almost systematically as high-risk activities, based either on the sector (border controls and the judiciary are included among the potential sectors for such classification), or on their intrusive nature (remote biometric identification, specifically).

11 Facial recognition, when sufficiently regulated, can also help to identify missing persons and terrorists at borders, or to build admissible evidence. Side-lining law enforcement agencies in the development and use of contact tracing applications for fighting COVID-19 is based on the same fears (mass surveillance risks). However, it would be important to involve law enforcement not for surveillance purposes, but to prevent the many risks of misuse by criminals.

there is scant focus on the role of internal security technologies in promoting the EU's digital sovereignty and leadership[12]; the data-driven economy raises challenges in terms of **competition and markets**, in addition to those relating to personal data, privacy or bias/discrimination; the European internal security industries are a strategic, future-oriented sector and a rich source of jobs and continuous growth[13];

- the **risks** of technological innovations limiting the operational capacity of police forces and the judiciary (such as 5G), given that criminal and terrorist groups are benefiting from them considerably (e.g. anonymisation), have been not assessed;
- the Coordinated Plan of the Commission and the Member States in the field of AI[14] included a **far stronger AI approach for security**, with three dimensions: i) enhancing the objectives of the security sector; ii) protecting AI technologies from attacks; and iii) addressing abuse of AI for malicious purposes.

In comparison, **cybersecurity is covered and emphasised more**:

- the White Paper correctly identifies it as one of the areas in which Europe is particularly strong: the data strategy describes it as an essential sector for investment and one of the key elements for ensuring the EU's digital leadership;
- the digital strategy makes it a key component of the Security Union, calls for the development of new tools for law enforcement and judicial authorities to combat cybercrime, synergies with cyber defence activities and support for the single market for cybersecurity;
- while ENISA is highlighted, none of the agencies in the justice and home affairs (JHA) sector - such as Europol, Eurojust or Frontex - are mentioned, despite their current and potential role in the fields of technological innovation and data.

---

12 Apart from a reference to robotics in the White Paper.

13 For example, according to the *Groupement des Industries Françaises de Défense et de Sécurité Terrestres et Aéroterrestres* (Group of French land and air-land defence and security industries), the French security industries account for 130 000 direct and indirect jobs and EUR 30 billion of turnover (50 % from exports), with an average growth rate of 5 % per year.

14 COM(2018) 795 final, 7 December 2018, *Coordinated Plan on Artificial Intelligence*.

The area of freedom, security and justice can only be achieved if the digital capacities of the justice and police services are enhanced under the Security Union and their needs are systematically incorporated in the various digital and industrial policies. This is all the more important in view of the increasing threats which may result from the COVID-19 crisis. The security industries should be one of the key sectors in the European economic recovery[15].

The Commission communications provide great potential for forming a genuine **public-private digital ecosystem for internal security**, if they are implemented in an integrated manner with the Coordinated Plan on AI and with the strategies adopted on industrial policy[16] and on digital partnerships, in particular the one with Africa[17].

This note sets out **12 recommendations grouped under five priorities** for enabling an ambitious implementation of the Commission proposals in the areas of internal security and criminal justice. The recommendations are explained in more detail in the Addendum.

Priority I. More actively support European technologies relevant for internal security

To speed up the digitalisation of internal security, the EU needs:

- an **industrial strategy for internal security technologies (1)**: driven by an overarching vision of the priorities, the strategy would bring together funding for research and innovation, experimentation and standardisation, including in the space and defence fields, with a view to developing sovereign sectors and relevant digital skills; it would involve mobilising public procurement and coordinating a European testing capacity to support the establishment of 'technological' policies and promote the competitiveness of European industries providing internal security solutions;

---

15 The document SWD(2020) 98 final of 27 May 2020, *Identifying Europe's recovery needs*, which accompanies the European recovery plan (COM (2020) 456 final of 27 May 2020, *Europe's moment: Repair and Prepare for the Next Generation*) identifies security as one of the sectors in which the EU needs to strengthen its strategic autonomy.

16 'Industry package': COM(2020) 102 final, 10 March 2020, *A New Industrial Strategy for Europe* (hereafter: 'industrial strategy'), and COM(2020) 103 final, 10 March 2020, *An SME Strategy for a sustainable and digital Europe* (hereafter: 'SME strategy').

17 JOIN(2020) 4 final, 9 March 2020, *Towards a comprehensive Strategy with Africa*.

- **smart regulation (2)**: enabling regulation, where it is needed, should ensure the protection of fundamental rights and freedoms, and support experimentation as well as the operationalisation of technological solutions; guidelines would reduce uncertainty and should enable innovative practices in the field of internal security. This approach would be facilitated by close cooperation between the law enforcement authorities, regulators and supervisors, with specific expertise for the latter and a flexible, pragmatic use of the General Data Protection Regulation (GDPR);
- **European data (3)**: a dedicated, closed data space, specifically for internal security actors, together with an open space for non-sensitive and miscellaneous data, involving the private sector and European research institutions, would speed up the development and uptake of European AI tools for enhancing internal security and protection of fundamental rights and freedoms. This would require robust mandates for the European agencies, particularly on processing of operational data for research, testing and algorithm-development purposes. Cross-referencing with other sector-based data spaces, especially in financial area, would also help improve internal security policies.

Priority II. Systematise risk prevention with respect to criminal use of technologies and avoid weakening of the capabilities of law enforcement authorities

The scale and speed of increasing risks from criminal use of technologies, together with the risk of greater impunity, require:

- **more rigorous integration of internal security in European digital and industrial policies (4)**: these risks will be accelerated by the spread of technological innovations, particularly those that are decentralised (such as cryptocurrencies and 5G). This cross-cutting approach would enable the implementation of '*privacy and security by design and by default*' and a rethink on our security approach to include raising awareness of innovators' communities to these risks and encourage them to find solutions. It would also reduce the risk of loss of operational capabilities by police forces and the judiciary;
- **strengthening the JHA agencies' cooperation with European cybersecurity structures (5)**: explicitly allow Europol to process operational data from CERT-EU directly; increase cooperation with ENISA and CERT-EU on vulnerabilities, to prevent organised crime groups from accessing cyber weapons and prevent terrorist groups from acquiring offensive capabilities;

- **developing secure digital finance (6)**: promote innovations in the field of digital finance in order to combat terrorist financing and money laundering, by preventing misuse of digital finance tools by criminal and terrorist groups; this entails reducing uncertainties regarding the interpretation of the GDPR by issuing guidelines and establishing a structured dialogue with the private sector.

Priority III. Rebalance the relationship between public authorities and the major digital platforms

In order to rebalance our relationship with companies that are mostly non-European and adapt the legal framework to address their actual responsibilities and liabilities, the EU will need to:

- **enhance the responsibility and strengthen the transparency of digital service providers delivering services in the EU, with regard to content and technological standards (7)**, bearing in mind the impact of their practices on users as well as on policies for preventing and combating crime and terrorism. The voluntary cooperation framework should be strengthened (EU Internet Forum) for better transparency and accountability of companies, and the EU as well as Member States should be more active in the Global Internet Forum to Counter Terrorism (GIFCT). The Digital Services Act package should increase the liability of companies for amplifying illegal content and include principles on legal harmful content; it should establish principles for transparency, assessment and monitoring of algorithms. Provisions on early collaboration with law enforcement and judicial authorities on standards as well as on allowing access to unencrypted e-evidence in response to a legal order, or on assessing potential risks of misuse of their technologies, could be adopted. These measures should enable the provision of better information to users, States and researchers, and improve the tailoring of public security policies. Particular attention should be paid to projects in areas that were so far the domain of the State;
- **establish European supervisory instruments (8)**, in particular by bringing together the various tools for combating illegal content (hate speech, terrorism) and disinformation, and defining a more assertive approach to legal harmful content, with a view to curbing the tendency of both types of such content to spread, in particular through the amplification effect of algorithms. Access to raw data of companies and internal research will help to carry out a more in-depth oversight.

Priority IV. Deploy an external strategy for digital partnerships and influence

Promotion of the European digital model for internal security should focus on:

- the **creation of common data spaces with key partners, and primarily Africa (9) -** which is a key partner of the EU with a strong take-up of digital. This could be done through the EU-Africa digital partnership[18] - and would be different from the models that have been actively deployed by our strategic competitors;
- **a strategy to build influence in international fora (10)** by bringing internal security issues in general digital policies spaces (e.g. the Global Tech Panel and the OECD), and intensifying cooperation on technologies with the international security organisations (United Nations and Interpol).

Priority V. Develop light, cross-cutting governance mechanisms to drive the digital ecosystem for internal security

The cross-cutting approach needed on technology and data requires more cross-cutting and flexible governance to enable the involvement of internal security actors:

- **developing an internal security Innovation Hub (11),** as an innovative and agile instrument that could contribute to the implementation of many of the recommendations at an operational level;
- **creating a strategic advice body on technologies and internal security (12)**, along the lines of the American National Security Commission on AI, which would supplement the cross-cutting work of the Security Union Task Force, to design a strategic vision in the field of internal security contributing to the EU's digital leadership and sovereignty.

***

The Commission will bear the huge responsibility of designing the EU's digital model. This model will affect the everyday lives of citizens, Member States and businesses, by deploying the benefits of digitalization whilst regulating against physical or legal risks.

[18] Such data partnerships would avoid "European bias" in the training of algorithms.

In a context of strategic tension, it needs to support our values and our industries in the EU and worldwide. It also needs to protect our democracies against the lethal threats of organised crime and terrorism, which are also benefiting from the digital revolution. It is therefore imperative that the EU develop a **flexible and pragmatic model that protects rights and freedoms as well as citizens, through the digitalisation of internal security and the integration of internal security in all policies with a digital dimension**.