Council of the European Union

Brussels, 8 July 2020
(OR. en)

9185/20
ADD 1

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 - Addendum

Harnessing opportunities to use security technologies, limiting risks and promoting the European digital model of internal security and criminal justice[1]

This addendum gives a detailed explanation of the 12 proposals, grouped under five priorities.

Priority I **<u>More actively support European technologies relevant for internal security</u>**

1. Develop an industrial strategy for boosting technologies relevant for internal security.

1.1. **Define technological priorities in the area of internal security:**

- identify the technologies and data which will be critical over the next five to ten years for the security of the EU's citizens and for its technological sovereignty[2], and for which the EU will want to play a leading role;

[1] For convenience, this addendum will use the term 'internal security' to cover criminal justice and the term 'criminal' to also include terrorism.

[2] The notion of sovereignty is to be understood as fostering own European digital and industrial capacities while keeping the EU open to external innovation and technologies under fair market environment. It will allow the EU to build these capacities and competences, as well as avoid creating "European bias".

- identify the next waves of innovation, for example biometric technologies and digital identity, encryption software that is resistant to quantum computers, technologies for the protection of personal data[3], the future of AI, space technologies[4] and technologies linked to 5G[5];
- adopt an overarching vision bringing together industry, trade and security, following the example of the EU's strategic competitors[6].

1.2. **Ensure that EU programmes and initiatives for research and innovation in digital /industrial areas cover internal security:**

- favour **multi-sector approaches**: numerous non-security technologies are used for public security (prevention, surveillance) or have the potential to be used in internal security[7]; many technologies are dual purpose (civilian and military); the convergence of certain technologies (e.g. AI and blockchain) should help avoid silos in public policy approaches;
- include internal security aspects in the **European Research Area** through the next Commission communication on the future of research and innovation and the European Research Area announced by the industrial strategy;
- make **substantial co-investment** with the Member States, in particular within the Digital Europe programme, as called for by the Coordinated Plan, for the deployment of AI services in security[8]. Internal security industries can play an important role in the post-COVID economic recovery;

[3] Use of synthetic data, anonymisation technologies, privacy-preserving machine learning (PPML) techniques such as federated learning or differential privacy, etc.
[4] For example, durable, altitude-resistant batteries (drones, robots).
[5] The EU must ensure it develops not only the 5G equipment manufacturers, but also the accompanying ecosystem.
[6] The 'Made in China 2025' plan (2015), for example, aims to position China as a world leader in ten industrial sectors, through a strong technological component, widespread public support for identified national champions, use of its trade policy, and the objective of autonomy in value chains.
[7] For example, AI technologies for video analysis or language or voice processing; for data processing, curation and enrichment platforms; and distributed and/or embedded AI.
[8] Annex to Coordinated Plan on AI, pp. 7-8: to prevent the malicious use of AI technologies for criminal activities or terrorism, and to better prevent, detect and investigate criminal activities and terrorism.

- mobilise the **European Innovation Council (EIC)**: include experts on internal security on its board and develop its networks of experts in this area[9]; strive to act increasingly as a **European venture capital fund in internal security**[10] to protect European players experiencing growth in strategic sectors[11], finance the start-ups and their scale-up for viable and strategic technologies, and help consolidate European businesses in a prioritised and selective manner.

1.3. **Promote, protect and consolidate our internal security industrial base to build European industrial sectors within the internal market:**

- **mobilise all European instruments**: trade policy (monitoring of foreign direct investment[12]), protection of intellectual property (future action plan)[13], competition law (in particular the fight against the abuse of dominant positions and tying practices for recommendation algorithms), taxation, support for venture capital focused towards internal security (future action plan on the capital markets union), support for exports, and support for financial innovation; **support via public procurement should be strengthened**[14];

[9] By connecting to the different high-level expert groups, the future industry forum, etc.
[10] Along the lines of the CIA's In-Q-Tel fund or the Israeli Libertad fund, which are based on a genuine economic rationale rather than purely on national interest.
[11] Even limited investment sends a signal of state interest which could avoid takeovers of European flagship companies using high tech in security applications, or foreign takeovers which would prevent European ecosystems from becoming consolidated.
[12] See in France the blocked takeover by an American company of Photonis, global leader in night vision.
[13] Intellectual property is a major issue in the data-driven economy: see the work done by the World Intellectual Property Organization (WIPO): https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=470053.
[14] Public procurement could play a role in ensuring the solvency of emerging European technologies in the field of internal security, by including this aspect in the selection criteria for procurement procedures, while keeping it of reasonable importance and avoiding to nurture dependence on public procurement.

- **limit the establishment of non-European data monopolies on security markets in Europe, including defence and space**, where non-European digital platforms are increasingly active[15] and could impede European players[16], in particular in the field of biometrics and identity security[17], which will take on a crucial importance in today's world of digital twins[18] and 5G. **New levers** such as the portability of industrial data[19] could help protect small European players;
- **monetise public sector data**, at a time of budgetary strain and considering tax avoidance by some non-European digital platforms, which are strengthening their position via free access to European data financed by public funds. The concept of 'data of general interest'[20] could usefully be developed further. While some data is meant to be public for free, other data should be shareable after payment of a fee[21].

1.4. **Promote European internal security standards in the future European standardisation strategy announced by the digital strategy:**

- standardisation is one of the most powerful tools for achieving **data sovereignty and technological leadership**[22]: our strategic competitors use standards related to security policy to support their technological industries and access European data[23];

[15] Amazon is providing a number of American police forces with facial recognition software, its GovCloud will host the Department of Homeland Security's biometric database and the company's CEO is very active in the space sector, Microsoft will be the Pentagon's cloud provider, Apple is investing in space technologies, while Google had to abandon Project Maven with the Department of Defense amid internal pressure, etc. The platform effect, whereby solutions with integrated or interoperable technologies can be produced for large numbers of users, is becoming dominant in a growing number of markets and is crowding out fragmented European players.

[16] The US platforms play a key role in encryption in particular, where under the guise of promoting the protection of personal data and cybersecurity they may be guided by protectionist considerations aimed at preventing other players from accessing the personal data on which they have built a dominant position.

[17] Google, Apple, Facebook, Amazon, Microsoft (GAFAM) and their Chinese equivalents regularly rise in the US National Institute of Standards and Technology (NIST) benchmarks and could quickly supersede the European flagship companies in these segments thanks to their giant databases.

[18] A digital twin is a virtual clone of a physical system or process.

[19] By providing model standard clauses or even imposing certain contractual clauses in legislation.

[20] Data which is private but obtained by companies as part of an activity linked to public authority (public service delegation, occupation of the public domain , exercise of a licensed regulated activity, etc.).

[21] Representative of the costs of data collection and processing, but without any economic added value.

[22] Report by Carl Bildt, *Calling The Shots - Standardization for EU Competitiveness in a digital era*.

[23] By creating entry barriers and obstacles for small businesses, the Financial Action Task Force (FATF) Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation championed by the US on cryptocurrencies penalise European industries specialised in blockchain and favour their competitors which have a critical size, and the 'Travel Rule' (virtual asset service providers will have to collect information on originators and beneficiaries of virtual transfers) opens up wide-scale access to European data.

- define measures to promote European internal security industries' products as **global standards for security technologies**[24], in particular by fully integrating the **protection of rights and freedoms**[25]: draw up priorities and methodologies, step up current work by European standardisation bodies in the fields of internal security, defence and space[26], and without placing an extra burden on SMEs and start-ups in particular; organise European lobbying within international fora (International Organization for Standardization [ISO], International Telecommunication Union working groups, Internet Engineering Task Force [IETF], National Institute of Standards and Technology [NIST], etc.) for standardisation projects deemed to be strategic[27]; it could be more efficient for the EU to finance a network of qualified, selected Member States and EU experts, independent from non-European economic powers, in support of Member States.

1.5. **Create a European testing and evaluation capacity for internal security:**

- this is a **missing link**: the EU does not have a capacity similar to that of the US Department of Commerce's NIST, which helps establish 'technological' policies and effectively boosts the competitiveness of American industry[28]: today, for biometrics, facial recognition[29] and analysis of digital traces[30], European police forces often have no alternative but to rely on NIST's work, which is of limited relevance in the European context, or to perform incomplete and costly internal assessments[31];

[24] Standardisation should be understood to cover formal standards as well as open standards.
[25] The work of the European Committee for Standardization (CEN) on the use of biometrics for automated border controls does not take account of European rules on the protection of privacy and personal data. The EU could champion standards which promote 'privacy and security by design and by default'.
[26] The CEN, the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI) conduct work on security (chemical, biological, radiological and nuclear, biometrics at borders, post-quantum encryption, etc.), cybersecurity, defence and space, in addition to work conducted in the digital field. There is a CEN-CENELEC security forum.
[27] For example, for 5G, meetings of national authorities were organised at Europol, then Commission funding was allocated to support European representatives' attendance at standardisation forums. See eu-LISA information note *Next steps for the development of the roadmap for standardisation*.
[28] NIST was founded in 1901 to address the weakness of US measurement capabilities compared to those of European rivals. NIST has a dual function: it manages overall consistency between standards and evaluates technology.
[29] In December 2019, NIST published a study drawing attention to wide-scale biases in facial recognition algorithms (see also https://www.nist.gov/itl/iad/image-group).
[30] https://www.dhs.gov/science-and-technology/nist-cftt-reports
[31] Facial recognition in public spaces must demonstrate its non-discriminatory and targeted nature (focused on perpetrators of serious crimes), by using careful and supervised testing to establish a framework for its use (temporary limited campaigns, camera quotas, placement on communication nodes, etc.).

- **promote the establishment and networking of national and European testing and experimentation centres for AI products and services in the area of internal security**, under the Digital Europe programme, to bridge the gap between research, innovation, (regulatory) experimentation[32], standardisation and market needs. This capacity would speed up the operationalisation of innovation[33], reinforce the competitiveness of European products[34] and boost the EU's technological sovereignty;
- the Commission's Joint Research Centre, which conducts numerous industrial tests, could coordinate this European network, in collaboration with the JHA agencies and the European authorities for the protection of personal data and fundamental rights;
- European data spaces and flexible regulation (see below) would facilitate the establishment of these centres which could contribute to the definition of European data format standards and would help to curb the brain drain of European talent.

1.6. **Bridge the gap between internal security and space and defence fields:**

- the synergies between civil and security technologies called for by the Space Strategy for Europe[35], the digital strategy[36] and the industry package[37] should lead to better synchronisation of research and innovation cycles in the areas of space and defence with those of internal security, e.g. between civilian European AI programmes and projects under the European Defence Fund and Permanent Structured Cooperation, as recommended in the White Paper[38];
- the future **action plan on synergies between civil, defence and space industries**, which was announced in the industrial strategy, **should take account of internal security needs and projects in research and innovation**[39], especially in robotics, as many technologies are dual use.

---

[32] See pages 8 to 10 of the annex to the Coordinated Plan; these testing facilities may include regulatory sandboxes.
[33] This is one of the goals of the Frontex Border Management Innovation Centre (BoMIC), for example.
[34] By enabling European companies, like their competitors, to offer technologies that are already operational or tested as a prototype .
[35] COM(2016) 705 final of 26.10.2016 *Space Strategy for Europe*. See in particular point 3.4.
[36] Footnote 4 mentions the Space Programme (but not the European Defence Fund).
[37] The industrial strategy lists the European Defence Fund and the Space Programme among the financial instruments that contribute to the competitiveness of European industry; the space and defence sectors, which according to the SME strategy are '*key for the EU's strategic and technological sovereignty*', offer major opportunities for European SMEs and start-ups through the European Defence Fund and the CASSINI space entrepreneurship initiative.
[38] Footnote 19 of the White Paper, although it does not cover AI for military purposes.
[39] For example by reinforcing existing links between JHA agencies and the European Defence Agency in AI, developing the role of the European Innovation Council in dual-use innovation or connecting Horizon Europe clusters 3 (civil security for society) and 4 (digital, industry and space).

1.7. **Invest in digital skills for internal security:**

- integrate the development of the digital skills needed in internal security into the updated digital skills strategy for Europe: support the **transformational effect** of AI and new technologies on professional cultures, organisations and process in the area of internal security[40], propose means of developing and maintaining the pool of **talent** needed in the EU, equip regulators and supervisors with **internal security skills**.

2. Adopt a regulatory approach conducive to innovation and competitiveness in the area of internal security.

The Commission's shift towards trustworthy AI rather than an exclusively ethics-based approach is positive because it opens up more uses while still integrating ethical aspects:

- laws should **both protect fundamental rights and freedoms and promote innovation and competitiveness in the area of internal security**[41], aiming for agility, the rapid dissemination of AI products, and the facilitation of experimentation through regulatory sandboxes[42];
- there could be a more flexible approach to regulation, for example in **research**;

[40] So that the spirit of innovation is instilled across the whole chain (including public procurement, for example).
[41] The White Paper recommends regulations which are innovation-friendly, conducive to rapid and widespread deployment of AI, and consistent with efforts to boost European competitiveness.
[42] The Coordinated Plan on AI supports these sandboxes as a way of ensuring that outdated or poorly adapted regulations, or the absence of regulations, do not hold back innovation. According to the SME strategy, they enable innovative solutions not already provided for in regulations or guidelines to be live-tested, with the appropriate conditions in place, with supervisors and regulators. The data strategy stresses a preference for experimentation (regulatory sandboxes), iteration and differentiation.

- **guidelines** for the public sector and internal security companies which favour the use of new technologies are crucial[43]: as indicated in the White Paper, it is primarily **legal uncertainty**, linked to the implementation of the General Data Protection Regulation (GDPR)[44], which discourages public use and undermines the competitiveness of European companies, which should not be put at a competitive disadvantage because of an overly cumbersome or unclear regulatory framework[45]; it is crucial that internal security authorities as well as private sector are playing a key role in the context of the development of such guidelines, which should use to a maximum extent the flexibility the GDPR allows[46]. In case legal obstacles or impediments arise nevertheless, it would be important to review the data protection legal framework to allow for the competitive development of AI in the EU;
- this smart regulation requires **diversification in recruitment** to include people with entrepreneurial and internal security backgrounds in regulatory departments and among fundamental rights and personal data supervisors, in order to bridge the gap between legal solutions and operational needs and constraints.

3. Harnessing common data spaces for internal security

The data strategy proposes the establishment of two spaces that are more directly relevant to internal security: a financial data space and a data space for public administrations, including to address law enforcement needs[47].

3.1. **Ease the use of data for internal security**:

[43] The UK's data protection authority (ICO) has published guidance explaining how to comply with the GDPR when developing AI algorithms. It supervises projects in very sensitive sectors (health, security, etc.), integrating data protection from the design stage and allowing for experimentation with robust safeguards in place (https://ico.org.uk/media/about-the-ico/consultations/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf). Guidelines should cover the field of digital finance.

[44] Some principles of the current data protection regime create some uncertainty with regard to potential impediments for the development of new technologies and enhanced use of data (e.g. data minimisation). A restrictive interpretation that would excessively curb the use of new technologies and data in internal security area would weaken public policies for public security and send an unfriendly signal to European industries. See COM(2020) 264 final of 24.6.2020 *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation.*

[45] See the relevant initiatives set out in the SME strategy, in particular the forthcoming Fit for Future Platform which will screen the existing EU legislation to identify potential for simplification and administrative burden reduction, or the role of the future high-level EU SME Envoy.

[46] As well as the future e-privacy regulation.

[47] The reference to law enforcement has disappeared from the French version of the document, but has been kept in the appendix.

- **facilitate the processing of operational data by JHA agencies**[48] for the purposes of research, development, testing, auditability and validation of AI tools for internal security, by including an explicit legal basis in their mandate[49]; operational data could significantly improve the accuracy of AI tools (reducing bias in facial recognition, detecting terrorist financing networks, etc.) as well as their competitiveness;
- establish a **data space specifically for the JHA sector** (JHA agencies, Commission and Member States): a data lake[50] or a more sophisticated platform would combine personal data (including pseudonymised data) and non-personal data (synthetic or anonymised data) to ensure the quality of the data and its accuracy for use in internal security, as well as prevent bias and discrimination[51]; the relevance of the use of operational data should be then assessed;
- set up **a data space for non-sensitive internal security data,** mainly for research purposes: the data, which can be openly shared, would originate from various sources and would be enriched by other type of data (e.g. space data); look into economic exploitation of the data[52] and facilitate its use by the JHA sector;
- foster **partnerships with industry for the use of data spaces**, primarily with European industries[53], in order to speed up innovation in internal security and so that European companies no longer have to train and develop their algorithms outside the EU (in particular for facial recognition).

These steps will require:

- a **clear and flexible governance framework for data spaces** so as to build trust and enable relevant data to be shared (determining what would be open data, data retention period and conditions, data formats, access rights and possible compartmentalisation, intellectual property for data sets, audits, etc.);
- a **sovereign infrastructure** capable of hosting the data lake securely;

[48] Operational data is understood by Europol to be data, personal or otherwise, that it processes under its mandate for investigative or strategic purposes.
[49] Aside from statistical or academic research purposes.
[50] A data lake hosts data without applying a schema to the incoming flows so that the data is immediately available and users can transform it according to their needs.
[51] AI tools trained and developed only with pseudonymised or non personal data sets are less accurate in general. The use of homomorphic encryption in the training process offers some potential to reach both precision and privacy.
[52] Monetisation of public data, free licence for public entities to use the technologies, etc.
[53] While avoiding creating "European bias" through datasets.

- **robust mandates for the European agencies**, in particular for the processing of operational data or data from the private sector[54], for the purposes of research, testing and developing algorithms, and for the exchange and pooling of data;
- **a legal framework**, designed with and for internal security authorities, to support the use of personal data (including pseudonymised data) and facilitating experimentation (regulatory sandboxes), with mechanisms to prevent bias and discrimination, that will help companies to develop products that include privacy and security by design and by default;
- **support for the creation of data reservoirs in the Member States, and the networking of them (between Member States but also with JHA agencies)**, with financial assistance from European programmes such as Digital Europe, which will help to improve the accuracy of data, the compatibility of data formats and to harmonise governance rules.

3.2. **Facilitate access to other sector-based data spaces for internal security (not only cybersecurity)**[55]**:**

- make use of the European **financial data space** to enrich business-to-government (B2G) in the financial sector, where public-private partnerships are a key asset in the fight against terrorist financing and money laundering (close cooperation between the private sector and financial intelligence units, Europol's public-private partnership for financial information), for the purposes of information exchange and innovation[56];
- open up non-personal data in the **other common data spaces** to those involved in internal security (operational actors, researchers, etc.): the field of health for better prevention of chemical, biological, radiological and nuclear risks in health facilities; mobility and energy so as to better protect ourselves against the risk of terrorist attacks on transport or critical infrastructure; the field of digital skills to identify internal security needs and adapt human resources policies;

[54] The scope of the data strategy does not include the sharing of privately-held data with public authorities (B2G – business-to-government) for its use '*for law enforcement purposes*', but the possibility is left open with a reminder that data protection and privacy legislation should be complied with (footnote 22).
[55] The digital strategy cites cyber resilience in the financial sector as an essential part of digital finance, and the data strategy stresses the importance of cybersecurity for energy.
[56] There are regulatory sandboxes in some Member States for innovative financial services (SME strategy).

- **avoid data silos**: if there is no common data pool, then non-personal data spaces should be interoperable, with a cross-sector approach taken to their use, to facilitate in particular strategic foresight efforts which require cross-referencing of non-personal data from a wide range of fields[57].

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

4. Mainstreaming the involvement of internal security actors in digital and industrial policies to identify risks at the earliest possible stage.

Security actors should be integrated into the planning and regulatory structures of digital policies, standards bodies and supervisors. This cross-cutting approach will make it possible to implement privacy and security by design and by default from inception.

4.1. Identify **risks of criminal use of technologies:**

- these risks affect **a large number of technologies and sectors** (e.g. the rapid progress of synthetic biotechnologies could make it easier for viruses to be produced outside laboratories through cloud labs)[58]; the decision to exclude the risks of criminal use of AI from the scope of the White Paper, while acknowledging the need to prevent it[59], is highly questionable;
- **these risks will accelerate with the spread of technological innovations:** open technology, anonymisation and decentralised technologies are needed to democratise access to technologies, offer highly innovative services and protect freedom of expression, but can also make these technologies more accessible to criminals[60];

[57] For example using climate data to anticipate the impact of climate change on the Sahel and reformulate the security responses accordingly.
[58] Similarly, contact tracing apps used for fighting COVID-19 should be designed taking into account the risks of data misuse and attacks which could render them inoperative.
[59] Footnote 7: '*Although further arrangements may need to be put in place to prevent and counter misuse of AI for criminal purposes, this is outside the scope of this white paper*.' However, the White Paper suggests that the concept of 'safety' covers cybersecurity and the malicious use of AI, which includes criminal intent, yet these are excluded from the general scope (see footnote 32).
[60] For example, the 3D printing plans for the 'Liberator' handgun were deliberately shared in 2013, or the open source software of 'privacy activists' Samourai, offering non-custodial (unregulated) Bitcoin wallets.

- these risks prompt us to **rethink our security approach**: anticipating convergence of technologies[61], preventing risks relating to access to knowledge of use as well as those relating to access to technologies, raising awareness about the risks among communities of innovators and promoting the search for solutions.

4.2. Anticipate the **risk of loss of operational capabilities of the law enforcement authorities**:

- in particular, studies concerning **6G** will have to take account of internal security needs in order not to repeat the experience of 5G, first apprehended from the sole perspective of market prices and then in terms of cybersecurity, omitting initially lawful interception[62];
- the EU should also define the 'European way' of regulating **encryption** with the aim of combining cybersecurity as well as privacy with access to data for the purpose of preventing criminal acts, conducting investigations and accessing digital evidence. Some of our key partners have already taken steps in this direction (see below)[63].

5. Strengthening cooperation between the European JHA and cybersecurity structures[64]**:**

- beyond the existing collaborative mechanisms[65], explicitly allow Europol to receive and process directly **operational data** from CERT-EU outside major incidents to improve the fight against the exploitation of cyberspace by criminals;
- **cooperate in the area of vulnerabilities** in order to prevent organised crime and terrorist groups from accessing cyber weapons: this cooperation would bring together deep knowledge about the cyber threat from the JHA agencies and knowledge from the cybersecurity structures (CERT-EU on operations and ENISA on strategy) about vulnerabilities and technical expertise needed to understand the attacks; this cooperation would build on a community of European actors involved in active searching for vulnerabilities, with a view to strengthening a European sector[66].

---

[61] https://i.unu.edu/media/cpr.unu.edu/attachment/3472/PauwelsAIGeopolitics.pdf
[62] 5G technologies make lawful interception more difficult without the adoption of standards enabling it.
[63] Note from the EU CTC 7675/20 (and ADD 1) of 8 May 2020: *Law enforcement and judicial aspects of encryption: The various forms of encryption*.
[64] The digital strategy suggests strengthening proactive mechanisms for information exchange to fight malicious cyber activity, synergies between civil cyber resilience, cyber defence and law enforcement, and new tools (page 6).
[65] CERT-EU, ENISA, Europol and the European Defence Agency have signed a memorandum of understanding, and crisis management mechanisms exist for large-scale cyber attacks; ENISA issues weekly reports on cybercrime and COVID-19, and Europol has set up a law enforcement emergency response protocol.
[66] Bug bounty groups (https://www.euractiv.com/section/digital/news/cedric-o-defends-french-covid-19-app-ahead-of-crunch-vote/); the question of the appropriateness of a commercial sector focused on vulnerabilities may arise.

6. Integrate the framework for combating terrorist financing and money laundering into the development of digital finance:

- the digitalisation of finance gives criminal and terrorist groups a large number of opportunities to finance themselves or conduct money laundering via social media, new payment platforms or cryptocurrencies[67];
- the **strategy on digital finance** announced in the industrial strategy should promote digital innovations and cybersecurity to combat the financing of crime and terrorism[68] and prevent the exploitation of technologies by these groups to finance themselves while hiding their traces, while at the same time protecting privacy; it should promote European standards to keep sovereignty over European data;
- the strategy should build on the **existing security framework** in terms of risk analysis[69], digital aspects of law enforcement regulations[70] and developments of the recent Action Plan[71];
- **support for technological innovations** should be facilitated by the common financial data space and guidelines for businesses to clarify the application of data protection and fundamental rights rules[72];
- a **structured dialogue with industries** providing these services and technologies (including blockchain) should be set up, in existing fora (EU Internet Forum) or in fora to be created.

Priority III <u>Rebalance the relationship between public authorities and the major digital platforms</u>

7. Increasing responsibility and transparency of social platforms and networks:

[67] RUSI Occasional Paper, *A Sharper Image: Advancing a Risk-Based Response to Terrorist Financing*, March 2020.
[68] The White Paper on AI states that the rapid deployment of AI systems is key for financial supervisors.
[69] Building on the Supra National Risk Assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.
[70] For example, the Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, the Directive on combating fraud and counterfeiting of non-cash means of payment, the Directive on harmonising the criminalisation of money laundering, and the Directive laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences.
[71] COM (2020) 2800 final of 7 May 2020 *Communication on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorism financing.*
[72] The Commission's Action Plan of 7 May 2020 suggests addressing issues of compliance with data protection legislation in the context of exchange of information between competent authorities (p. 7).

- the **Digital Services Act** package should update **the regulatory framework of digital service providers** to increase their responsibility and ensure **supervision of their policies** on **content management and standards**[73], to rebalance the existing asymmetry of information;
- public trust in digitalisation must be based on robust safeguards in terms of individual rights and freedoms, as well as on the accountability and transparency of such digital practices, which should benefit citizens, states and researchers[74];
- in terms of **illegal content**, the limited liability laid down in the 2000 e-commerce Directive ('mere conduit' principle) is now outdated in terms of the true impact of algorithms and technological choices on users and public policies to prevent and combat violent extremism and terrorism. Although these companies often present themselves as staunch defenders of privacy and freedom of expression against state intrusion, their practices may help amplify extremist or illegal content;
- **technological standards** may inadvertently serve criminals, e.g. anonymisation techniques that can foster impunity, or the widespread encryption of communications that could have an adverse effect on lawful interception; ambitious projects such as Libra, which are aimed at disrupting the current monetary system, raise questions about the implementation of the existing rules on money laundering and terrorist financing[75];
- the **voluntary cooperation framework** (EU Internet Forum) should be strengthened, to support more transparency and accountability from companies delivering services within the EU with regard to their practices and research activities; the EU should be active in the working groups and research activities of the Global Internet Forum on Counter Terrorism (GIFCT)[76];

[73] The digital strategy converges with the White Paper (which proposes reconsidering the allocation of liability between actors along the whole supply chain of algorithms, from the developer, via the provider, to the user).
[74] See also the recommendations made by the High-Level Expert Group on Artificial Intelligence or reflections such as *Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims*, April 2020.
[75] See Statement by the French G7 Presidency on stablecoins of 17 October 2019.
[76] The new statutes tend to dilute the role of governments and therefore that of the EU. The GIFCT finances the Global Network on Extremism and Technology, a research network on the use of technologies by terrorists.

- the **Digital Services Act package** should enhance the liability for illegal content and could design principles regarding legal harmful content[77]; it should increase the transparency, assessment and monitoring of algorithms[78] in order to monitor digital services providers' implementation of their obligations, to assess the impact of algorithms (e.g. recommendation systems), or to encourage innovations (e.g. content detection tools)[79]; general principles could be set out therein concerning the obligations of digital service providers to cooperate with law enforcement and judicial authorities at early stage on standards, as well as to allow, in response to a legal order, access to electronic evidence that is readable and unencrypted[80], or even provide an assessment of the risks of misuse of their technologies.

8. Set up stronger supervision mechanisms:

- the Digital Services Act package should bring together and strengthen the current disparate mechanisms for combating illegal content (hate speech, terrorist content) and disinformation, given their common dynamics (companies involved, propagation channels, and the ideological proximity of certain content), in order to secure rapid and adequate results;
- the supervision of technology standards would seek to reconcile innovation, cybersecurity and the protection of individual rights with preserving law enforcement and judicial authorities' access to data for carrying out their tasks;

[77] Legal harmful content is a content that does not cross the legal threshold but which is or could be particularly damaging to consumers, especially vulnerable users; its amplification might fuel radicalisation even of violent nature (see https://www.gov.uk/government/consultations/online-harms-white-paper).

[78] The White Paper on AI proposes an ex-ante assessment, a continuous monitoring system and ex-post controls on high-risk AI systems, in particular through testing, auditing or certification, based on access to data or documentation, and the verification of actions or decisions that may have been taken by AI systems.

[79] There should be an examination of what risks and opportunities the measures adopted for SMEs to restrict compliance checks would bring to small platforms in which organised crime and terrorist groups are active.

[80] Demand made in a recent joint statement by European police chiefs concerning 5G; See abovementioned Note from the EU CTC concerning encryption (7675/20 (and ADD 1) of 8 May 2020): *Law enforcement and judicial aspects of encryption: The various forms of encryption).*

- it would pool the resources of the current cooperation framework[81] for the purpose of conducting in-depth technical work, e.g. on the policy for dealing with legal harmful content, or the amplifying effects of recommendation algorithms[82], based on companies' raw data and access to internal research work.

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

9. In addition to the removal of barriers to the flow of data and the promotion of an ethical AI as an international standard, support for **data partnerships related to internal security with like-minded countries that endorse the EU's approach,** in particular in **Africa**:

- Africa is a region where the uptake of digital technologies has been particularly rapid, Africa is a key partner for the EU, especially in the area of security;
- the digital partnership with Africa outlined in the digital and data strategies should deploy **common data spaces for use in internal security**, notably in the area of facial recognition and automated language processing[83]. Such data partnerships would also avoid "European bias" in the training of algorithms. Joint work on universal data standards could be appropriate;
- the EU-Africa strategy recommends that the digital partnership should cover the prevention of internet use by terrorist and violent extremist groups online. It also suggests collaboration in the field of AI and space (data and technology), which could also be beneficial for internal security;
- this partnership should **respond to the entryism of our strategic competitors**, who arrange access to security technologies in exchange for personal data, in particular biometric data, exporting their political model in the process[84];

[81] EU Internet Forum (terrorist and extremist content), High Level Group on combating racism, xenophobia and other forms of intolerance (illegal hate speech), Multistakeholder Forum on Disinformation Online (disinformation).

[82] The digital strategy announces a European Democracy Action Plan and a specific action plan for the media and audiovisual sector to promote an open and democratic society. In order to combat political manipulation, the White Paper recommends assessing the use of algorithms in the prioritisation of information available to consumers and content moderation. In addition see the impact assessment of the Digital Services Act Package.

[83] A dual-use project (security/non-security) on the automatic processing of languages, both written and spoken, would be particularly relevant given the linguistic diversity of both Europe and the African continent and the potential for applications (voice command is a fundamental field of machine autonomy and a tool for digital inclusion).

[84] China's digital model (*social credit*, framework for political freedoms, etc.) is part of its 'Digital Silk Road' (see the example of Zimbabwe in the area of facial recognition). Google inaugurated an AI research centre in Ghana in 2019; Amazon sold its facial recognition for customer identification tool Rekognition to a financial services company operating in West Africa.

- this partnership could build on the European Union-African Union Digital Economy Task Force and make use of CSDP missions to identify the potential of data to be shared and technological solutions needs.

10. Develop an influence strategy in international fora:

- bring the European internal security agenda to the **major international digital fora** in which the EU is involved, in particular the Global Tech Panel steered by the HR/VP, as well as the Internet Governance Forum, in the OECD and in initiatives such as the Global Partnership on AI[85];
- develop cooperation with the **United Nations system**[86] **and Interpol** on the use and risks of new security technologies.

Priority V <u>Develop light, cross-cutting governance mechanisms to drive the digital ecosystem for internal security</u>

11. Swiftly establish the EU Innovation Hub for Internal Security in order to gradually implement many of these recommendations **at operational level**[87]:

1) carry out a **risk assessment** on the criminal use of technologies (including by terrorist groups) and implement strategic foresight;
2) play a **leading role in research and innovation**: help to identify priorities for critical technologies for EU security; identify potential sources of EU funding, in better synchronisation with space and defence; support pilot projects with industry partners and in close collaboration with the European standardisation organisations;

[85] Initiative launched in June 2020 following the Global Forum on AI for Humanity held in Paris in October 2019, with the aim of creating an international regulatory agenda on applied AI (France, Germany, Italy, Slovenia and the EU are founding members, together with Australia, New Zealand, Canada, the UK, the US, Mexico, India, Singapore, Korea and Japan).

[86] In particular UNOCT and UNICRI (Centre for Artificial Intelligence and Robotics). These two entities also signed a draft strategic partnership in September 2019.

[87] 5757/20 of 18 February 2020 and 7829/20 of 7 May 2020, *EU Innovation Hub for Internal Security*, approved by COSI. For a longer-term development, see the EU CTC notes in 9069/19 of 8 May 2019, referred to above, and 6158/20 of 19 February 2020, *Embracing new and disruptive technologies in internal security and justice with an EU Innovation Hub*.

3) establish a **data space for internal security** and identify opportunities for use for the internal security of data of other spaces;
4) together with the authorities responsible for **protecting fundamental rights and personal data protection**, co-develop regulatory sandboxes, practical tools in the form of guidelines or recommendations for the use of AI systems, and research topics; set up a supervision mechanism for use in internal security;
5) ensure the **involvement of the internal security stakeholders** (Member States and European agencies) **and European security industries** in the Commission's digital and industrial actions (6G, etc.); recommend relevant actors for effective and coordinated representation in European and global processes (standardisation, certification, regulatory processes, etc.);
6) contribute to the setting-up of a **testing and assessment structure** for technologies used for internal security.

It will not initially be possible for the Hub to be involved in all these activities, but it should be able to take them on gradually. It is imperative that European agencies and Member States are able to quickly supply human resources to the Innovation Hub. The Commission should identify the financial programmes from which the Hub could benefit[88].

12. Establish strategic guidance on technologies for internal security to supplement the cross-cutting action of the Security Union Task Force:

- it is important that the future **Security Union Task Force**[89], steered by the Secretary-General of the Commission, plays a cross-cutting role in integrating digital internal security challenges into the actions of the Commission's Directorates-General, in the framework of the Security Union Strategy;
- following the model of the Horizon Europe Security cluster, these actions should be supplemented as necessary by mainstreaming internal security, ideally with the presence of internal security competences in the Directorates-General responsible for digital and industrial policies, and in new structures that could emerge with the Digital Services Act package;

[88] Such as the Digital Europe programme, but also other forthcoming initiatives to support SMEs and start-ups (e.g. developing the future EU Startup Nation Standard).
[89] In the field of defence, space and industry, the creation of DG DEFIS is a significant step forward.

- set up **an equivalent to the US National Security Commission on Artificial Intelligence (NSC AI)**[90] **to shape a strategic vision for new technologies for internal security**: made up of figures from the public sector, academia, and the private, civil and defence sectors, its studies and recommendations are aimed at US leadership in AI in the fields of security and defence. This expert advisory body would make it possible to draw up priorities and formulate strategic proposals (industry, internal and external) and to contribute to the alignment of European research, innovation and financing[91], standardisation and regulation efforts in the field in the field of internal security. It would suggest some innovative ways to allow regulation to cope with the speed of development of technologies and digital practices.

---

[90] https://www.nscai.gov
[91] The head of In-Q-Tel is a member.