Council of the European Union

Brussels, 3 June 2019
(OR. en)

9069/19
EXT 1

CT 47
COSI 99
CATS 70
ENFOPOL 217
TELECOM 207
CYBER 146
COMPET 381
RECH 247
CFSP/PESC 365
CSDP/PSDC 235
HYBRID 14
RELEX 481
ESPACE 47
IND 167

NOTE

From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	Disruptive technologies and internal security and justice

Introduction

Convinced of the need to rapidly put the internal security sector in a position to benefit from digitisation while minimising the risks associated with it, at the beginning of April 2019, with the support of the General Secretariat of the Council (GSC), the European Commission and a number of European Union (EU) agencies, the EU Counter-Terrorism Coordinator organised an informal seminar at 'thecamp', a campus in France dedicated to innovation.

The seminar, held over two days, afforded the opportunity to some 40 senior officials of the GSC, the Commission, the Parliament, the main EU agencies and the European Data Protection Supervisor (EDPS) to exchange views with around 15 experts in disruptive technologies, which are innovations that transform parts of the economy. The main lessons set out below can be drawn from the seminar.

This paper is meant as a contribution to the debate about mobilizing new and disruptive technologies for security and justice, as well as fully assessing their risks. While developing European leadership in this field will be a medium-term process, a number of immediate next steps could be taken.

1. Acceleration of the use of new technologies in the area of internal security

New technologies represent as-yet underexploited potential in the area of internal security, as regards detection (weak signals indicating cyber attacks, border reconnaissance or terrorist financing flows, etc), prediction and analysis (use of big data, for example to prevent radicalisation) and exploration or operational response (offensive capabilities in cybersecurity). The Commission adopted an ambitious package for cybersecurity in 2017. The work DG HOME has launched on the use of artificial intelligence (AI) for security is a step in the right direction.

1.1. A European vision of medium-term priorities for new technologies in the area of security is urgently needed. Technological revolutions are often driven by large non-European digital groups. The EU is capable of accomplishing major joint projects (Galileo). **It is vital that the EU decides on the security technologies in which it wishes to play a leading role over the next five to ten years and then takes steps to implement this vision**[1]. **The EU needs to invest in the next waves of technology and innovation**, in which it can lead rather than merely playing catch-up.

[1] China for example is strengthening its industry to become a global leader in new technologies; the 'Made in China 2025' plan is interesting to consider in this context.

1.2. The EU also needs **sovereignty over its data**: too many European companies, particularly those involved in the area of facial recognition, train their algorithms in China because of the ease of access to data; developing synthetic data or promoting European datasets, the auditability of algorithms or AI that is less dependent on personal data are all avenues to explore.

It would be important for the EU to define its own **standards** for access to the market for facial recognition or post-quantum solutions.

Civilian/military cooperation at European level would be key for the development and exploitation of new technologies, in particular with regard to specific large-scale projects such as Galileo.

The EU would also need to **develop a real foreign policy for data**: in addition to promoting our own datasets, a **major partnership** as an alternative to the increasing Chinese facial recognition offerings would be a considerable asset for the EU.

2. Systematic assessment of the risks and threats arising from new technologies

By its nature, digitisation brings with it systemic risks. The vulnerability of citizens, economies and governments increases proportionately to their connectivity and interdependence, and could rocket due to the arrival of 5G technologies and connected devices. There is now greater awareness of the scale of cyber threats. In addition, **it is important for the EU to fully understand and anticipate the threats posed by technological innovations**: these may in fact be old technologies whose development has speeded up as a result of new capabilities.

2.1. For instance, **compromised data** (deep fake, fake evidence, hacking, social or political manipulation, etc.) today represent one of the greatest risks to an AI economy, and soon, quantum computers will be able to break any encryption, synthetic biology will enable viruses to be recreated with ease outside of the laboratory and the human body or connected devices could be weaponized. **Social, economic and political changes have the potential to completely disrupt the existing frameworks for ensuring security**: possible scenarios like absolute transparency would allow every citizen to constantly monitor police activity, blanket data protection would render security services blind, there could be a shift towards privatised security or a new form of terrorism could emerge in response to technological developments.

2.2. The digital world functions as an ecosystem in which **the private sector - particularly the large, foreign technology groups but also globalised communities of individuals - drives innovation** fuelled by a concentration of talent, infrastructure and capital. **Besides, many of today's technological revolutions are silent** because they take place away from the public gaze. The huge growth in synthetic biology, driven by the reduced cost of genome sequencing, the very high value of human capital and an abundance of funding give rise to technology which is less complex to handle and more accessible on open source. This **democratisation of technology is not without risk**. Globalised communities of innovators share a belief in the benefits of opening up technology and in their capacity to regulate themselves. Thereby potentially leaving the door open to malicious usage, as demonstrated by the widespread use of cryptocurrencies by criminal groups.

2.3. Moreover, **numerous projects using decentralised technologies aim at circumventing or weakening States**, in order to reappropriate market power for the benefit of individuals, including in the area of functions that have until now been reserved for the State. For instance, in the area of proving identity, States are now in direct competition with large online companies (which aim at delivering 'silent identification' via their interfaces) or banking consortia. This may soon be the case in the areas of health, education and even security.

2.4. Finally, the **internet's multi-stakeholder governance model** raises a number of security-related questions. The difficulty which the private non-profit institution ICANN (Internet Corporation for Assigned Names and Numbers) has in allowing satisfactory access to the WHOIS registers by law enforcement and police authorities and the lack of priority regarding lawful interceptions within international working groups on internet governance or 5G standards demonstrate the need to address security issues in a more proactive manner in these types of fora.

3. Further developing the European governance framework for technology

Various recent Commission's initiatives in the fields of digital single market, digitizing European industry, cybersecurity, defence, space to support development of new technologies are welcome and important. There are growing numbers of civilian and military agencies in the field of technological innovations in the Member States.

3.1. The EU may need to **further develop and adapt its governance in the technology fields to be suited to the pace of innovation.** It is important to be able to identify the next waves of security technologies, quickly release sufficient capital with the freedom to fail, encourage tests and prototyping, and decide quickly whether to accelerate or give up, aiming for industrialisation from the outset. This methodology would be akin to that adopted by the US defence agency DARPA (Defense Advanced Research Projects Agency), whose work has resulted in major industrial and technological achievements in both the civilian and military spheres. In that respect, 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.

In parallel, considerations of urgency require that **a considerable proportion of the principal technological and investment programmes** (e.g. Horizon Europe, Digital Europe and InvestEU, etc.) within the next Multiannual Financial Framework **be earmarked for security** (Challenge 7, relating to security and freedom, accounts for just under 2.5 % of the Horizon 2020 programme).

3.2. It may be necessary for the EU to **work in a more integrated manner**, with the support of the Member States. This updated form of governance would allow for cluster working, bringing together entrepreneurs, researchers, funders, the public sector, civil society and the private sector. It may also ensure **better synchronisation of security investments with military investment**, including in the space sector, which is one of the key factors in the success of the United States and China in becoming leaders in the information economy.

3.3. Finally, this updated governance may require a new way of creating and applying **data protection rules to new technologies, taking security interests fully into account**. Data protection regulations are indispensable for building the Security Union and giving back to Europeans sovereignty over their data, but they should not become obstacles in principle. It is important that a **modern European framework for personal data encourages the emergence of new technologies,** including for security. The mandates of the agencies may need to be modernized in this context.

4. Building a joint innovation lab for the European agencies

The European Justice and Home Affairs (JHA), cybersecurity and defence agencies are technology platforms that are already available for use by the Member States. They have advanced technical skills and possess a substantial pool of data. The **creation of a joint innovation laboratory for JHA agencies (the 'lab')**, under the leadership of Europol and with the strong support of other relevant agencies such as Frontex, Cepol or Eurojust, would provide a real catalyst for innovation in internal security. It would bring together the relevant European and national elements of the public sector (institutions, agencies, the EDPS), academia, the private sector (startups, from small enterprises to large corporations), and the civilian and military sectors across the entire value chain (research, investment, production), with a view to developing products for the market. This laboratory would have the following tasks:

4.1. Constantly **evaluating the risks and opportunities presented by new technologies**, with the help of the Member States and other relevant stakeholders. The laboratory would raise awareness of the risks among the different communities of innovators and would engage in long-term forecasting work. The lab would identify business needs of the law enforcement and judicial communities in relation to new technologies (e.g. admissibility of e-evidence, predictive police…).

4.2. Creating a **shared data lake** for the agencies in which the data would be reliable, monitored and used to train AI tools. This would go beyond interoperability of the existing databases. A trusted European data infrastructure (cloud), coupled with an ability to structure upstream data, would bring real added value to the simple development of software tools. The laboratory could work on **standardising data** for the agencies. It could conduct **simulations** of the misuse of technologies, along the lines of cyber labs.

4.3. Securing access to and the use of data **in legal terms with the help of the Commission and the EDPS**. Since security, privacy, safety (industry) and transparency of algorithms (ethics) may be conflicting concepts, **the lab could offer a deconfliction mechanism for dealing with operational cases**. In parallel, the lab could start work on principles and technological tools with the EDPS, researchers and internet companies, with the aim in particular of exploring pseudonymisation technologies for data transfers, anonymization technologies for data retention, and the potential of differential privacy, or of producing specific guidelines for the internal security sector. Specific ethical rules should also be made available by the laboratory, including in training, by harnessing the work carried out at European level. The Joint innovation lab would also facilitate the collection via Eurojust of information on the legal challenges encountered in particular in the field of admissibility of evidence (i.e. reliability of evidence put in question by new technologies, role of chain of custody and cross-examination).

4.4. Planning the necessary transformations within the agencies to attract **talent** and create new **jobs**, for example in data analysis, algorithm creation and control, data infrastructure management or data labelling. This would also involve developing new methods of cooperation between academic talent or the private sector and the security professions, which are themselves expected to evolve. Attracting such talent will involve offering opportunities which combine issues of public interest with access to exclusive data or technologies. The transformations of the public sector would need to include a discussion on **future recruitment requirements** and a definition of innovative **training** and **management** arrangements for security practitioners.

4.5. Initiating **pilot projects**, in accordance with the 'DARPA' method described above, with the necessary flexibility. The use of blockchain technology could be trialled, for example to assist the Europol/Eurojust joint investigation teams, or to create an alternative to informal hawala-style messaging for the transfer of migrants' funds or to ensure the traceability of antiquities in order to prevent them being trafficked for the benefit of terrorist organisations, on the basis of existing blockchain solutions and in partnership with regional or global players (e.g. the World Bank).