Council of the
European Union

Brussels, 18 September 2019
(OR. en)

12224/19

LIMITE

COSI 184
ENFOPOL 400
CYBER 257
JAI 949

NOTE

From:	Presidency
To:	Standing Committee on Operational Cooperation on Internal Security (COSI)
Subject:	The future direction of EU internal security: new technologies and internal security - Preparation of the Council debate

Introduction

At the JHA Council meeting in June 2019 and the informal COSI meeting in July 2019, detailed discussions about the future of EU internal security took place, raising a number of topics that will require further, more focused discussions. One of those topics was 'disruptive technologies', and the Presidency intends to continue the debate on relevant threats, challenges and opportunities. The overarching aim of the these discussions is to put European law enforcement in a position to benefit from major new technologies, while anticipating and minimising the risks associated with them.

The introduction and increased use of new technologies unquestionably poses a threat to the legitimate needs of the law enforcement sector. In general, facing the challenges which new technological innovations cause for criminal investigations is a complex and many-sided problem that is not only limited to criminal proceedings. Also, the legitimate need of individuals, companies and authorities to protect their information must be taken into consideration. Therefore, it is important to identify the relevant threats, challenges and opportunities that come with the new technological measures, as well as to find a balance between efficient criminal investigations on the one hand and the protection of fundamental rights and data protection on the other.

Key technology trends with the most significant impact on internal security

1) 5G mobile networks

5G is likely to complicate lawful interception for law enforcement, criminal investigations and justice. Due to the high security standards of 5G, and a fragmented and virtualised architecture, law enforcement and judicial authorities may lose visibility on valuable data, such as the content of communications or identification of users, including the location of devices, or this access could be seriously hindered. Similarly, the integrity of data and its admissibility in court proceedings may be compromised. The above risk is mainly linked to features such as network slicing, increased use of end-to-end encryption and the encryption of the 'IMSI' number.

On the other hand, the arrival of 5G may also bring significant opportunities for law enforcement. For instance, with its high reliability and low latency, 5G may offer great potential for replacing conventional radio communications in order to ensure mission critical communications (MCC), provided that it is kept safe from cyberattacks, especially 'denial of service' attacks (e.g. cutting power to entire communities).

A thorough assessment of these challenges and law enforcement needs, including the impact of 5G networks on the interception capabilities of law enforcement authorities, could therefore be necessary. If needed, this assessment could feed into the ongoing 5G standardisation process to ensure that the standards comply with national legislation, e.g. on providing the possibility for lawful interception.

2) Artificial Intelligence (AI)

AI and robotics have the potential to transform law enforcement by enhancing its efficiency and responsiveness in several different ways. AI may acquire and analyse large amounts of information gathered from a multitude of data sources, devices (cf. Internet of Things below), tools and applications, which would not be possible via human intervention only. AI may save substantial resources for law enforcement by enabling automation in many different areas.

The availability and use of AI-backed technological tools is likely to become indispensable for law enforcement, but there are serious legal, ethical and technological constraints to be taken into account. It will be of crucial importance to ensure that the user remains informed and in charge instead of becoming an oblivious observer. Outcomes proposed by AI technologies will be based on a varying degree of probability, and as such, they will require critical assessment and verification or validation by humans. The recent rapid advance in the field has outpaced the corresponding ethical reflection, leaving open the question of what precisely the concept of transparency could and should mean in this context. For example, in addition to using AI for lawful purposes only, the data sharing and processing framework must be designed in a way that adheres to the principle of purpose limitation. The development of AI ethics into a discipline of its own should therefore be encouraged.

3) Internet of Things[1]

The Internet of Things uses a variety of different software and hardware products as well as communication standards and connectivity protocols. Combined with the large and constantly increasing number of connected devices, this creates a broadened surface for attacks and increases the number of attack vectors.

For law enforcement, the Internet of Things presents specific investigative challenges due to the diversity of hardware, software and communication standards and connectivity protocols being used. Some of the relevant data may be located in the Cloud, which will frequently require cross-border cooperation and legal assistance.

Accessing, extracting, identifying and combining the relevant evidence (i.e. digital forensics) will routinely become a Big Data problem, requiring major investment in skills, tools and expertise on the side of law enforcement.

[1] EDOC # 830746 v2 Cybersecurity and the Internet of Things – a Law Enforcement Perspective, by EUROPOL

4) Drones and other Unmanned Autonomous Vehicles (UAVs)

The threat posed by drones is likely to continue to grow as they become more widely available, affordable and capable. The drones of tomorrow will be smaller and quieter, but also more powerful, as they will be able to fly further and carry larger loads thanks to lighter and more efficient batteries, increased data storage and computing capacity, smarter software and the introduction of 5G.

Moreover, the threat is not a hypothetical one: drones are already being used to smuggle illicit goods over borders, to disrupt the functioning of airports or to target individuals, police forces and other government authorities, as well as critical infrastructure. Also, by way of example, incursions into prison facilities and over borders occur regularly.

On the other hand, the technical development of drones is providing a new set of tools for law enforcement. Police forces and other government authorities currently use drones in different ways and the use of them is growing.

5) Anonymisation and encryption

Criminals regularly make use of online anonymity and encryption tools – such as Virtual Private Networks (VPNs), Tor and Darknet forums – to avoid detection and localisation, allowing them to operate in a relatively secretive environment. The importance of this phenomenon is increasing as we encounter a new generation of offenders that has grown up with technology and is extremely comfortable using IT. At the same time, most of these technologies have over time become much easier to use, and using VPNs or Tor requires very little technical skill.

Many social media and online messaging applications now have end-to-end encryption (E2EE) embedded by default in their design, which means that even offenders without any technical skills can communicate under relative anonymity. An appropriate reaction to this threat requires computational power, tailored technical solutions, skilled and numerous human resources and a clear legal framework.

It is important to find the balance between, on the one hand, public order, internal security and providing law enforcement with access to encrypted networks and, on the other hand, the protection of fundamental rights, such as privacy and confidentiality of communications, while also taking into account the principles of necessity and proportionality. In addition, the legitimate business interests of service providers, data protection aspects and customers' legitimate needs to protect their privacy and information and to protect themselves against crimes such as identity theft and corporate espionage must also be taken into account.

6) Other technologies on the rise

Despite their various stages of advancement, several other areas of technology could already be identified as potential future threats, but possibly also as opportunities in the area of law enforcement and internal security in general.

Amongst them, 3D printing is likely to increase criminals' access to weapons and tools previously requiring complicated technological procedures and entailing significant and often prohibitive costs. The materials used are also likely to compromise traditional detection methods, thus doubling the threat.

Another area to be mentioned here is biotechnology, which opens the way for fraud and manipulation with human DNA or other biometric features. Impacts on the collection and reliability of evidence could be tremendous as the technology advances and becomes more easily accessible to criminals (cf. the abovementioned simplification of access to anonymisation and encryption on the internet).

Main areas of internal security architecture influenced by new technologies

The above areas of modern technology will have a significant impact on many aspects of internal security as we know them today.

Amongst them, operational policing and cross-border police cooperation holds a prominent place: the exchange of data will be heavily influenced by increased automation and the ever-growing demand for interoperability and standardisation of data and technologies.

Besides being a threat, the use of drones and other devices limiting human involvement may also present an opportunity for law enforcement (e.g. reducing the danger for police officers in high-risk operations), but they will require new skills.

The possibility to analyse and process large amounts of data will offer opportunities for 'predictive policing'. Better reliability of facial recognition, automatic number plate recognition and similar applications will significantly enhance the capabilities of law enforcement.

In terms of communication, the arrival of a new generation of mobile networks may start a gradual replacement of traditional radio communications by communications based on a 5G or 6G network, offering better cross-border compatibility and fast and reliable reaction times.

Main challenges related to the above

With the above said, all the stakeholders involved also need to be aware of the challenges to be monitored and solved with respect to new technologies.

In meeting the legitimate needs of society for a high level of security, it is important to strike a balance between empowering law enforcement and preserving fundamental rights, also taking into account the principles of necessity and proportionality. The legitimate business interests of service providers, data protection aspects and customers' legitimate needs to protect their privacy and information such as confidential communications must also be taken sufficiently into account.

Limitations in the current legal framework are obvious and include issues such as profiling or the current challenges facing Europol in processing personal data obtained from private parties. In the same vein, the fact that the EU is a leader in the protection of personal data imposes very strict requirements on law enforcement. The anonymisation of WHOIS data after the entry into force of the GDPR is a prime example.

From a technical point of view, lawful interception of mobile communications and other relevant data will constitute another major challenge. Similarly, the transparency and correctness of algorithms used in all applications of artificial intelligence as well as other appropriate safeguards need to be looked at in order to maintain the ability to verify the credibility of the results proposed and to ensure the overall accountability and lawfulness of such algorithms.

Finally, rapid advancements in technologies used by both criminals and law enforcement will require a structured and long-term approach to the training of police forces, and to human resources in general, so that law enforcement becomes attractive for professionals with the necessary skills. Allocation of corresponding financial resources will be an absolute requirement in that context.

Way forward

In June, Ministers stressed that the future of EU law enforcement lies in investing in innovation and technology and harnessing their potential, while maximising the use of available resources. Priority should be given to pooling equipment, know-how and resources, specialised capacity building and tactics, and enhanced partnerships with the private sector. This would allow for common policing solutions tailored to the evolving needs of Member States' authorities.

By way of example, the Member States seem to broadly agree on the need to explore the creation of an overarching structure dedicated to innovation and technologies so that EU law enforcement can become a truly proactive player regarding the impact of those technologies on internal security.

In order to translate this goal into specific action, the delegations are invited to discuss the following questions:

Do you agree that:

- the Innovation Lab to be created at Europol should monitor and drive technological developments to ensure that EU law enforcement is in a position to address these developments at an early stage? What other tasks should the Innovation Lab fulfil in order to meet those broader objectives?
- existing structures dealing with technology in law enforcement, such as the ENLETS network, should be strengthened and possibly integrated into the above Innovation Lab?
- the needs of law enforcement should be systematically taken into account across relevant sectors of technology, such as in the case of 5G and lawful interception, including in impact assessments conducted by the Commission?
- action should be taken in order to enhance the dialogue between law enforcement and the private sector, including in relation to Europol, with the possibility of legislative amendments at EU level?