Council of the
European Union

Brussels, 30 September 2019
(OR. en)

12496/19

LIMITE

COSI 199
ENFOPOL 415
CYBER 263
JAI 984

NOTE

From:	Presidency
To:	Permanent Representatives Committee/Council
Subject:	The future direction of EU internal security: new technologies and internal security

Introduction

At the JHA Council meeting in June 2019 and at 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 - the new or ‘disruptive’ technologies - has now been discussed in further detail at the September COSI meeting, raising questions requiring guidance at ministerial level.

The overarching aim of those discussions on the threats, challenges and opportunities brought about by new technologies is to put European law enforcement in a position where it plays an active role and is able to benefit from major new technologies, while anticipating and minimising the risks associated with them. It is important to note that new technologies influence all authorities and EU agencies involved in protecting our internal security.

Taking into account the role of law enforcement and judicial authorities in securing cyberspace as a safe environment for citizens, it is important to ensure security and the authorities' operational needs when developing new technology such as 5G. Moreover, the introduction of 5G networks will have multiple security implications, for instance in relation to data security and critical infrastructure. The EU's common 5G security risk assessment and the forthcoming toolbox have an important role to play in terms of securing our future networks

Overview of previous discussions

Previous discussions were based on a series of Presidency documents[1] and valuable contributions by the EU Counter-Terrorism Coordinator[2] (EU CTC), identifying not only the most important technology trends to be monitored, such as 5G mobile networks, Artificial Intelligence or encryption and anonymisation, but also the increased use of drones and other unmanned aerial vehicles, the risk of fraud with biometric features thanks to biotechnology and the possible misuse of 3D printing.

That said, technological developments also present a series of interesting opportunities for law enforcement, for instance in the fields of automation and interoperability, facial and number plate recognition or predictive policing based on the analysis of large quantities of data.

From a legal point of view, it will be important to strike a balance between empowering law enforcement and preserving fundamental rights and the protection of personal data, also taking into account the principles of necessity and proportionality.

Way forward

The above areas of modern technological development will have a significant impact on many aspects of internal security as we know them today. The limitations of the current legal framework are obvious. They include issues such as profiling or the current challenges facing Europol in terms of 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 strict requirements on law enforcement.

[1] 9393/19, 12224/19

[2] 8983/19, 9069/19

As stressed in the ministerial discussion in June, the future of EU law enforcement lies in investing in innovation and technology and harnessing their potential, while maximising the use of available resources. Prioritisation of pooling equipment, know-how and resources, specialised capacity-building and tactics, and enhanced partnerships with the private sector would allow for common policing solutions tailored to the evolving needs of Member States' authorities. This should be supported by a structured and long-term approach to the training of law enforcement.

Based on the discussion in COSI, the Member States support the creation of an overarching structure at Europol dedicated for example to analysing any developments in this field, innovation and research, and dialogue with the industry and academia, so that EU law enforcement can become a truly proactive player in terms of the impact of technological developments on internal security. This structure could take the form of an Innovation Lab.

At the same time, Member States called for a better definition of the tasks and priorities of such a Lab, and pointed out the need to address the financing of any new assignments.

Conclusion

In order to define the way forward on the basis of the discussion, delegations are invited to discuss the following questions:

Do the Ministers agree that:

- it is essential to adopt a coordinated approach on how to address the threats, challenges and opportunities brought about by new technologies, in order to ensure synergies and avoid overlaps between different actors, such as national authorities and different EU agencies,
- the Innovation Lab to be created at Europol should monitor and drive innovation, including the creation of common technological solutions in order to pool scarce resources and generate savings,
- the Innovation lab should bring together law enforcement with academia and existing actors in the public sector and,
- 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.