Council of the
European Union

Brussels, 22 November 2019
(OR. en)

14297/19

LIMITE

COSI 239
ENFOPOL 508
ENFOCUSTOM 196
FRONT 333
DAPIX 346
CYBER 322
JAI 1217

NOTE

From:	Presidency
To:	Permanent Representatives Committee/Council
Subject:	Future direction of EU Internal Security - Outcome of discussions - Presidency report

The rapidly changing security environment requires an integrated approach to address new threats and challenges. A comprehensive approach to internal security is a viable way of addressing threats that are more complex and varied than before, enabling a whole-of-society approach to the responses provided.

In implementation of the Strategic Agenda 2019 - 2024 in the field of Justice and Home affairs, the Presidency has run a series of thematic discussions to deepen reflection on the way forward regarding the future direction of EU internal security. The Presidency has outlined three fundamental principles to guide these reflections: offering an area of freedom, security and justice to its citizens; combating social exclusion and discrimination; and promoting the Union's values.

The discussions were launched in July 2019, at the informal meeting of the Standing Committee on Operational Cooperation on Internal Security (COSI), in preparation for the informal Justice and Home Affairs Council (JHA Council), by raising a number of key horizontal topics[1]. Thematic discussions also took place in the relevant working parties, such as the Law Enforcement Working Party (LEWP), the Terrorism Working Party (TWP) and the Working Party on Information Exchange (DAPIX IE), and were further prepared at COSI for the ministerial debate. A number of topics were addressed in detail, e.g. enhancing the operational cooperation framework for law enforcement, impact of new technologies and hybrid threats on internal security, role of the EU JHA agencies, information management and automation, and training for LEA. The detailed strands of these discussions are presented in the papers produced for the various meetings and listed in the annex to this report.

This report covers selected aspects, reflecting the Presidency's view on the key issues that emerged from these debates to be carried over to the legislative cycle 2019-2024.

1. Proactive approach to new technologies

Technological developments have a major impact on the life of EU citizens and subsequently on law enforcement work. All these developments, such as artificial intelligence, unmanned aerial vehicles, new communication networks and online environments, to name just a few, can support the work of authorities, but can also be used for illegal purposes. For example, both law enforcement and first responders can make use of drones, such as in counter-terrorism work and respectively in the aftermath of a terrorist attack. The increasing pace of innovation challenges the capacity of law enforcement agencies to adapt to the rapidly developing technological world. In the context of digitalisation, it would be necessary to assess the extent to which the legal frameworks in which law enforcement authorities and relevant EU agencies operate correspond to the current needs[2]. Preserving and promoting fundamental rights should underpin any such developments, while respecting the strict requirements on law enforcement activities, deriving from the framework of data protection, where the Union has a leading position in standard setting.

1 Presidency paper on the future direction of internal security in the EU (WK 13264/19)
2 Documents 12496/19 and 12224/19, New technologies and internal security

The aim is to give EU law enforcement a proactive role in order to be able to benefit from new technologies, while anticipating and controlling the risks associated with them. There is a need for an integrated, comprehensive approach at EU level in this field. The creation of a joint innovation lab within Europol to harness technological developments and trends, innovation and research, and to assess their potential relevance for law enforcement and dialogue with the industry and academia supports this aim. Full exploitation of new technologies requires constant research and training. Centralising certain activities and pooling together the results of the work of existing networks, within the innovation lab, would bring benefits in terms of rationalisation and cost-efficiency, especially in areas where Member States do not have sufficient resources to act alone or where there is added value in acting together and exchanging best practices.

As technological research and development often take place in universities and the private sector, law enforcement authorities are involved at a relatively late stage. In order to take into account law enforcement authorities' concerns for the future, the Presidency considers that efforts should be made towards involving law enforcement authorities proactively in the technological development processes from the start, notably by further enhancing the participation and the coordination of law enforcement practitioners in EU funded research and development programs for security.

The Presidency encourages law enforcement authorities to be proactively involved in the development of new technologies. The innovation lab should function as a platform to support this aim. It is important that the needs of law enforcement authorities are known and taken into account at an early stage when developing new technologies that influence their work or that are required for a more effective law enforcement response. Moreover, internal security and law enforcement interests should be better taken into account in legislation related to new technologies in order to mitigate limitations in the legal framework, in particular through addressing them systematically in threat assessments.

2. Effective information management

Law enforcement cooperation at EU level will increasingly be based on better and more efficient technological solutions and information systems and their interoperability[3]. In an era of large volumes of digital data, law enforcement authorities have access to more data and information than ever before. This needs to be reflected in the technical solutions and capacity on offer. At the same time, key statistics on various crime areas are missing. Therefore, it is particularly important to ensure that information systems are supplied with high-quality and complete data and used effectively. We must ensure that relevant national authorities have access to these systems and are sufficiently trained to enable their full use.

Criminal analysis remains at the core of law enforcement. Analysis provides the added value to raw data that turns it into actionable information that can be used nationally, as well as in cross-border operations across the EU. However, a clear vision of EU-level standards for crime analysis work is lacking and needed. At any rate, analysis is an integral element of all information processes within law enforcement. This necessitates sufficient human and financial resources to process and analyse information. The successful enhancement and standardisation of analysis therefore requires a better understanding of law enforcement needs as a whole and of the various information processes involved in particular, including those of criminal investigation and criminal intelligence gathering.

The Interoperability Regulations[4] entered into force on 11 June 2019. Ensuring the efficient implementation of the Regulations is critically important. This technological revolution of EU IT systems will require a great amount of resources and compliance with the timeline, both at EU level and in the Member States. While building the interoperability architecture, it is important that technical solutions always take into account the needs of the end-users. In addition, it is crucial to provide appropriate and continued training for end-users in order to be able to use these new information systems and complete their interoperability. It is clear that interoperability is much more than developing IT systems; it also involves a change of mind-set. Therefore, the successful implementation additionally requires a change in our operational and administrative cultures.

---

3 Document 13510/19, EU Information management – automation, access to, exchange of, and analysis of information.

4 EU 2019/817 and EU 2019/818.

On a broader scale, enhanced information exchange is not only a technical development. To achieve the desired benefits, it needs to be ensured that competences, resources and end-user interfaces at the national level are fit for purpose. Information is not an absolute value; it needs to be usable and lead to action. Without proper implementation, these developments and their benefits may be jeopardised.

Next to effective investigation, law enforcement authorities' work should be equally focussed on preventing and disrupting crime. Effective, high-quality information in the right place and at the right time contributes to this objective. With regard to intelligence-led law enforcement, Europol and Frontex are in a prime position to support this work with their analytical capabilities, including by having wider access to the Schengen Information System (SIS), as long as the Member States systematically provide them with high-quality raw data.

The Presidency calls for a comprehensive EU information management framework, in order to ensure that all the necessary existing information is accessible, processed and exchanged quickly and efficiently so that it gives rise to action in an intelligence-led way.

3. Multidisciplinary cross-border cooperation

Enhancing cross-sectoral operational cooperation through reducing duplication and increasing effective coordination is a key to successful action. Due to the constantly evolving, cross-cutting nature of various security threats, such as CBRN weapons and hybrid activities, the actions taken to respond to and prevent these activities require a horizontal approach, while taking into account the competence of Member States in matters of national security. There is a need for an integrated and coherent approach to ensure multidisciplinary operational cooperation, going beyond cross-border law enforcement cooperation, thus involving also other authorities, such as civil protection actors.

Differences in national decision-making processes, legislation and operating models are major challenges to operational cross-border cooperation. Moreover, inconsistencies in national data collection and processing practices, resulting from differences between individual Member States in terms of administrative systems, technical solutions and functional arrangements, hinder cross-border cooperation. Another challenge involves identifying and removing the obstacles to operational cooperation between law enforcement authorities, such as addressing incompatible radio frequencies in border areas, language barriers and the need to supplement existing legal bases with more detailed bilateral agreements. In urgent situations, national entities may not be aware of the range of operational alternatives – which are fragmented into several EU instruments – and information exchange channels available.

Multidisciplinary operational cooperation between law enforcement authorities should be intensified by developing and using new methods of working together and exchanging information, while relying on new technological applications and tools. These applications may include, for example, unmanned autonomous systems, automatic number plate recognition technologies or single-search interfaces for available databases. There is clear momentum and opportunity to continue and further support this development.

Lifelong learning and training is even more important in exploiting all existing possibilities and preparing for future challenges. The training provided by the EU agencies must be used efficiently. At the same time, it must be ensured that the activities of EU agencies complement each other and that overlaps are eliminated.

We must take into account regional differences and national specificities, while aiming for a common law enforcement culture among EU law enforcement authorities. Improving language skills, learning each other's cultures and exchanging best practices help to better understand regional and cultural differences and support the common goal.

Bilateral and multilateral arrangements remain important for local and regional cooperation and flexibility is needed in ensuring respect for regional diversity and different operational interests. Defining the division of responsibilities, jurisdiction and sovereignty need to be taken into account in any future developments.

The EU JHA agencies continue to play a significant role in supporting Member States' efforts within their respective mandates. It is widely accepted that a true cross-border cooperation between the authorities of the Member States, strongly supported by the relevant EU agencies, is the most viable way to proceed towards a Security Union and to address both existing and new threats in an ever-evolving environment in a sustainable way[5].

Future developments in the area of internal security would thus require a continued active role for agencies, involving an expected increase in the volume of existing tasks and new responsibilities, deriving from both political and operational needs. Given the resource limitations, there is a need to discuss the context in which agencies can create added value most effectively, e.g. areas where Member States might need to gain access to resources or technical equipment through pooling of resources, where data analysis capacities could be enhanced, and where stronger operational support could be provided. Transparent criteria should be established for deciding in which areas the Member States need most support, taking into account technological advances and specific material or other resource needs. When developing the role of the agencies, the aim should be a balanced solution that takes account of Member States' needs. It is essential to apply a coordinated and holistic approach in order to enhance the core expertise and strengths of each agency as well as to create added value in a cost-effective manner and without creating overlaps in tasks and functions.

There is a need for deeper agency-based information sharing and cooperation, as the existing and emerging threats in internal security are becoming increasingly complex and cross-border in nature. There is also a need for more effective interaction with private parties in the framework of information sharing. In particular, there is a need to assess Europol's legal base to request and receive personal data directly from private parties[6].

---

5 The role of EU agencies has been specifically addressed at the iCOSI and ICouncil in July, WK 13271/19 and WK 13266/19 and has been a cross-cutting theme through all debates

6 Discussions on Europol's cooperation with private parties have taken place at LEWP: docs. 10494/19, 11832/19, 12858/1/19.

In order to strengthen Europol's multidisciplinary approach to law enforcement in the long run the cooperation between Customs authorities and Europol should continue to be developed by increasing the number of Customs liaison officers in Europol, promoting the use of SIENA by customs in all EU Member States, and enhancing regular and structured information exchange between the parties including risk management and intelligence information. A short term goal should be to strengthen Customs contribution and integration to the implementation of the EMPACT OAPs. These actions would continue the positive development in the cooperation between customs and Europol of recent years.

The challenges in the cooperation between the European Union and Interpol need to be addressed. It is important that databases that serve as major information sources for law enforcement cooperation with third countries remain in effective use by the EU Member States' authorities in the future. At the same time, the applicable data protection legislation naturally needs to be fully respected.

The Presidency underlines the need for a review of the legal framework for cross-border law enforcement cooperation and the Europol's mandate in order to adapt it to current realities and future challenges. The development of a common law enforcement culture among EU law enforcement authorities should be further supported.

4. Comprehensive approach to security

A number of trends and developments can be expected to take place in the near future that will affect the threat landscape in the EU. Crime continues to be driven by demand as well as the availability of opportunities for criminal ventures. Furthermore, security changes in the neighbouring regions and various forms of violent radicalisation in Europe continue to pose a threat to our internal security. A comprehensive approach to security with better coordination, resources and technological capacities requires a better situational awareness and preparedness for a variety of challenges.

Law enforcement, civil protection and other relevant authorities should continue to develop their preparedness to counter hybrid threats. Cooperation on preventing and countering hybrid threats between relevant national authorities, based on their respective mandates, as well as EU institutions, bodies and agencies across the internal-external security nexus, needs to be continuously improved and mainstreamed. At the same time, it is important that synergies are increased and the duplication of efforts avoided, including through horizontal working methods, increased information exchange, and training and exercises cutting across sectors.

The need to continue discussions on the internal dimension of hybrid threats, particularly on the roles of JHA agencies in bolstering the EU's and Member States' capabilities to identify hybrid actions and their sources, is emphasised.

Moreover, the effective tackling of disinformation requires a comprehensive approach. In this vein, the participation of the law enforcement authorities, including in existing EU mechanisms, such as the Rapid Alert System, should be considered. Law enforcement authorities enhance the resilience of the EU and its Member States, and tackling disinformation needs to be taken into account[7]. The Presidency stresses the need for the better use of existing tools and the enhancement of holistic coordination at EU level. JHA agencies' support for Member States' also needs to be addressed in this context.

The use of technology and the internet in orchestrating criminal activities will continue to grow. For example, the use of online platforms on both the surface web and the dark web for trade in a wide array of illicit goods is expected to increase. Furthermore, the online sphere can be misused effectively to radicalise, recruit and incite to violence. The dissemination of terrorist and child abuse content online should be efficiently prevented and the relevant content taken down swiftly.

[7] Hybrid threats and internal security: Law Enforcement Strategic Communication and Tackling Disinformation (11831/19).

Moreover, the role of the prevention of violent radicalisation as an integral part of a comprehensive approach to fighting terrorism is highlighted. Engaging with and supporting first line-practitioners continues to be key in preventing and tackling violent extremism. There is a need to address politically or ideologically motivated violent extremism in all its forms. Henceforth, the focus on countering and preventing violent extremism and terrorism should continue to be forged using a broad-based approach, also taking into account the emerging trends in violent extremism.

The threat posed by right-wing violent extremism and terrorism needs to be tackled through creating a better situational overview, continuous sharing of good practices, cooperation with key third countries, and addressing the spread of unlawful right-wing extremism content both on- and offline. The challenge of returning foreign terrorist fighters should be addressed, including through the more efficient use of the SIS.

The Presidency underlines the need for a comprehensive and whole-of-society approach to security in order to address various threats to internal security. The importance of working across all relevant policy sectors in a more strategic, coordinated and coherent way is underlined.

ANNEX

Subject	Meeting	Reference Number
Future Direction of internal security in the EU	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13264/19
Hybrid threats and internal security	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13265/19
Twenty Years of Europol - what next?	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13266/19
The future of EU Internal Security	Informal Council meeting on 18-19 July 2019, Helsinki	WK 13271/19
The future direction of EU internal security: new technologies and internal security	JHA Council on 2 October 2019	12496/19
Hybrid threats and Internal Security	JHA Council on 2 October 2019	12495/19
Right-wing violent extremism and terrorism	JHA Council on 2 October 2019	12494/19
EU Information Management - Automation, access to, sharing of, and analysis of information	COSI meeting on 19 November 2019	13510/19
The future of EU law enforcement: Training for law enforcement	COSI meeting on 19 November 2019	13973/19