Future direction of internal security in the EU

Introduction

At the JHA Council in June Ministers had a first exchange of views on certain aspects with horizontal implications for orienting future developments in the area of internal security and EU law enforcement in particular[1].

As announced at the Council, the Finnish Presidency intends to take this debate further building on the EU Strategic agenda and in the context of the renewal of the EU institutional cycle. This will be done among others by bringing up thematic discussions on various aspects in the area of internal security, migration and justice to deepen the collective reflection on these matters. The objective is to consolidate the outcome of these discussions by the end of the year and to confirm the position of the Council on the future direction in the JHA area.

Internal security is and should be addressed as part of a yet bigger picture. We should talk about comprehensive security that encompasses a number of different issues, phenomena and challenges, such as climate crisis, military threats, natural disasters including extreme weather events, scarcity of energy and water resources, population growth and population movements, terrorism, infectious diseases, serious and organised crime and its manifestations, such as drug and human trafficking, cyber attacks and hybrid threats that have an impact on the overall vulnerability of our societies. A comprehensive approach to internal security is a more viable way to address threats that are more complex and varied than before enabling a whole-of-society approach to the responses provided. The social dimension of security, e.g. integration of all members of the society and fight against poverty, social exclusion and discrimination, play a vital role in the prevention of a variety of security related problems as well as necessity to respect human rights and rule of law.

The Finnish Presidency underlines that security should be viewed as a chain with judicial cooperation through each phase. In order to balance our actions, developments in law enforcement should be reflected in judicial cooperation and vice a versa.

Future direction of internal security: challenges and needs

In the past years the EU security environment has seen rapid changes, notably due to a number of crises in the neighbouring regions, such as the conflict in Ukraine, the civil war in Syria, terrorism, polarisation and the migration crisis.

The purpose of this paper is to outline certain horizontal themes, which the Presidency considers important for defining the future direction of internal security in the EU towards an effective EU security union. The paper builds on the debate of Ministers at the June Council and details the work streams highlighted by Ministers, e.g. stepping up the integrated approach to security; ensuring that internal security actors are in a position to benefit from digitalization and

[1] 9393/19

technological developments, while increasing the preparedness of law enforcement to the security risks coming with it, or ensuring the effective implementation of adopted measures, with a particular focus on the implementation of the interoperability package.

The paper also introduces additional aspects that in view of the Presidency should be considered in defining the next steps in internal security. It also outlines the concrete follow-up that the Presidency would like to provide on some of the general issues identified in the next six months, including by means of dedicated thematic discussions.

Consistent with this approach, a thematic discussion on enhancing the operational cooperation framework for law enforcement is put forward in the second part of the paper.

1. Effective implementation

As already stated at the June Council, there is a need to intensify the implementation and application of EU legal acts and measures, while taking into account that the implementation process is resource-intense and generates additional workload for the relevant stakeholders. For instance, connection of Europol to the Visa Information System, full implementation of the Prüm Decisions and of the PNR Directive, as well as transposition of the most recent EU legislation in the field of firearms must be achieved. Resources, including the necessary technical and expert capacities, need to be put together to support Member States in their efforts, including financial and organisational support at EU level.

In view of the Presidency, there is also a need to better monitor and assess the effectiveness and implementation of EU legislation. Once we have an overview of the impact of EU acts and measures, or the practical issues encountered in their implementation, it will be easier to assess the need for new initiatives and continue developing targeted measures.

The few existing evaluation mechanisms, e.g. the mutual evaluation mechanism pursuant to the Joint Action 97/827/JHA of 5 December 1997[2], on the application and implementation at national level of international undertakings in the fight against organised crime run in the Council, provide valuable insights on the practical application of various instruments. We need to draw more systematically on the results of these evaluations for developing better targeted policy solutions in the area of internal security. COSI could play a steering role in this context. Consideration could be given to a Schengen-type mutual evaluation and monitoring mechanism in the area of corruption and organised crime, in order to improve trust between Member States in this area.

2. Technological developments and internal security

Technological developments have had a big impact on the life of EU citizens and subsequently on law enforcement activities. The increasing pace of innovation challenges the capacity of law enforcement agencies to adapt to a rapidly developing technological world.

Law enforcement work is information-based activity. Information is gathered, processed and acted upon in order to prevent, detect and investigate crime. For law enforcement to be effective, large

[2] Joint Action of 5 December 1997 (97/827/JHA), OJ L 344, 15.12.1997 pp. 7 - 9.

quantities of information or data collected from a variety of sources, are required. In this regard, digital tools, AI and robotics are well suited to transform law enforcement, by enhancing how efficiently it can acquire, analyse and act upon the information. It is even conceivable that, with the increased proliferation of sensors, internet of things (IoT) and growth of big data, law enforcement may become heavily reliant on AI and robotics in the near future in its daily work. This is in particular the case for the fight against cybercrime, for which access to and the analysis of electronic evidence is crucial. The cooperation amongst authorities, and between authorities and other entities that often operate the technical infrastructure, is also crucial in that regard, all the more when technology is moving towards an end-to-end encryption environment.

Security of communication channels has become vital for our society. Disruption of the integrity, confidentiality or availability of transmitted information or even the disruption of the service itself can seriously hamper everyday life, societal functions, economy and national security. Communication infrastructures are the cornerstone of our societies, with 5G networks as the building blocks of a new digital environment. This requires resilient communication infrastructures and services, as well as technical standards and cooperation channels that allow authorities to respond effectively to crimes targeting these infrastructures and services.

Full conformity with the guarantees for fundamental rights and freedoms as laid down in the EU Charter of Fundamental Rights, the European Convention on Human Rights and related case law, including EU rules on personal data protection need to be ensured - and enforced.

The Presidency intends to continue a thematic discussion on this matter to look more in depth in the issues presented by digital transformation in the area of internal security[3].

3. Information management for internal security

Law enforcement cooperation at EU level will increasingly be based on better and more efficient technological solutions and information systems as well as their interoperability.

In the coming years (2020-2021), the upgraded existing systems (SIS, VIS, Eurodac), the new systems (EES, ETIAS, ECRIS-TCN), and the interoperability between them will gradually enter into operation. Effective implementation of the regulations[4] on interoperability is key.

It is particularly important to ensure that information systems are used effectively and supplied with high quality data. We must make sure that relevant national authorities have access to these systems and that EU agencies, including Europol, obtain all the information and data they require to carry out their tasks most efficiently. When enhancing EU information systems and their interoperability, it is also crucial to ensure that the solutions chosen will sustain the border control process without significantly obstructing the smooth functioning of border checks.

Arriving at a successful interoperability model would also require structural changes in the Member States to ensure that new processes of interaction between the competent authorities

[3] In its paper on *Disruptive technologies and internal security and justice* (9069/19) the EU CTC has identified a number of issues and possible next steps related to the impact of technological developments on internal security that could support a more detailed consideration of these issues.
[4] 5691/19

are put in place and effectively managed. This could be supported by providing regular oversight on recurring issues as part of the discussion on the future of EU information management. The latter was highlighted in the context of the debate launched by the Romanian Presidency in DAPIX IE, with regard to cross-border information exchange. The Finnish Presidency will continue this debate. Furthermore, the debate on automation of data exchange processes, such as explored in the ADEP/EPRIS project, should also be pursued.[5]

In addition, as far as further development of EU information systems and interoperability solutions are concerned, they must take into account the information currently excluded from the scope of the interoperability regulations, such as data covered by PNR[6], Prüm[7] and FIUs or the customs databases to make a complementary use of centralised and de-centralised systems.

4. Collecting, exchanging and analysing information

In the era of digital data, law enforcement authorities have access to more data and information than they can use. IoT, for example, will further multiply the sources of information available. The need to ensure that law enforcement authorities are in a position to use digital data and large volumes of information and to boost the effectiveness of crime analysis was underlined at the Council in June.

A clear vision of EU-level standards for crime analysis work is needed. However, analysis is an element of all information processes within law enforcement. A successful enhancement and standardisation of analysis activities 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 acquisition, management (including exchange) and analysis of information should be governed within a single legal framework.

A prerequisite for a reliable and sustainable data management process is a systematic improvement of the quality of data supplied to information systems and databases. In the framework of implementing the information management strategy, eu-LISA carried out a project on enhancing data quality, which deserves a follow-up.

Furthermore, the role of biometric identification should be further intensified in the prevention and investigation of crime and in issuing identity documents. It is becoming increasingly easy and inexpensive to fabricate deceptively accurate-looking digital images and video. We need to anticipate this threat by improving the methods used to identify false imaging, including by training staff.

Systematic monitoring and analysis of risks at the external borders is a key to enhancing capacities for early warning, decision-making and early response. To improve border security, which is instrumental for increasing internal security, it is important to ensure the development of state-of-

[5] ADEP (Automation of Data Exchange Processes) is the name of action 2 on the 5th IMS action list of the Working Party on Information Exchange and Data Protection (DAPIX), which is currently running the EPRIS-ADEP (European Police Records Index System) pilot project.
[6] Directive (EU) 2016/681 of the European Parliament and of the Council.
[7] Council Decision 2008/615/JHA.

the-art risk analysis products for the national, regional and local levels in all Member States in accordance with the CIRAM risk analysis model[8], which the Member States are required to use. These risk analysis findings could support building enhanced analytical capacities at Europol in its capacity as the EU law enforcement information hub.

5. Multidisciplinary approach between authorities

Internal security is a broad and comprehensive concept. Cooperation between public authorities, including police, customs and border guards, social and healthcare sectors as well as judicial authorities, is crucial. Cross-sectoral cooperation between authorities at national and EU level makes it possible to rationalise the use of funds and resources available nationally and for international cooperation, and to apply them in a mutually beneficial manner in order to face complex threats.

To ensure complementarity between the measures taken by the Union and its Member States, efficient use should be made of the multiannual strategic policy cycle for European Integrated Border Management and the related national and Frontex plans, as well as the measures available under the multiannual financial framework. In this process, cooperation between the authorities should be considered broadly to avoid creating obstacles to practical cooperation between law enforcement, border, customs and rescue authorities and to prevent a separate development of management systems or surveillance capacities. The multiannual cycle should be used to establish an interoperable, unified and continuous process for border security and return practices.

When attending to Europe's internal security, we must make use of the synergies already in place in the fields of law enforcement cooperation and criminal justice systems and make sure that they complement and reinforce each other. Maintaining internal security requires the entire process of criminal procedure, from criminal intelligence, criminal investigation and prosecution to handing down and enforcing sentences, to function smoothly. Particular attention should be devoted to crime prevention.

Capacity building should be considered strategically and across different policy sectors, drawing on identified risks and critical needs at EU level in the context of EU Civil Protection Mechanism. The upgraded Mechanism will be complemented with rescEU, an EU-level capacity created to provide assistance in overwhelming situations. These are situations where overall existing capacities at national level and those pre-committed to the European Civil Protection Pool are not able to ensure an effective response to the various kinds of disasters faced by Member States

6. Follow the money approach

"Follow the money" approach should be more systematically integrated in relevant initiatives and activities, at both policy and operational levels as an essential tool to effectively respond to evolving criminal landscape including terrorism financing.

[8] Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016, Article 11.

The impact and security risks associated with the use of cryptocurrencies and new means of payment should be given particular attention. To secure the integrity of the financial system and to address such security risks, it will be of paramount importance to maintain a structured interaction with the financial regulatory and supervisory actors or standard setting bodies, including European Central Bank, European banking authority and FATF.

Sufficient resources, expertise and judicial support should be made available to support financial investigations in Member States. Swift access by the competent authorities to relevant information is of fundamental importance when it comes to the effectiveness and speed of financial investigations. In addition to the establishment of beneficial ownership registers and centralised bank account registries foreseen under the EU Anti-Money Laundering Directives, the new Directive facilitating the use of financial and other information provides the competent authorities and Asset Recovery Offices with direct access to bank account information. This will significantly improve the capacity of these authorities to carry out financial investigations. In this respect, pursuant to the provisions of the 5th Anti-Money Laundering Directive, the Commission also has to submit a report assessing the conditions and the technical specifications and procedures for ensuring secure and efficient interconnection of the centralised bank account registries.

Moreover, it is essential to recover the proceeds of crime in order to ensure that “crime does not pay”. The Commission is expected to deliver by end 2019 a report on the implementation of the confiscation Directive (2014/42/EU), which might be accompanied with further proposals.

Increased support for financial investigations at EU level is needed, with an ever more important role to be played by Europol. The possibilities offered under the EMPACT OAP on Criminal Finance, Money Laundering and Asset Recovery should be used to their full extent. The Future European Financial and Economic Crime Center at Europol will help further consolidate the efforts in this area. It would be also appropriate to reflect how to reinforce and possibly streamline the activities of Europol's FIU as well as the work and activities of the networks as such, and to promote the use of the FIU.net or of its possible successor.

7. Training for law enforcement

Developing knowledge is a time- and resource-consuming process, and law enforcement authorities need to optimise the use of their resources, people skills, organisational experience and services provided. The EU Strategic Training Needs Assessment (EU STNA) conducted by CEPOL identified EU level training priorities in the area of internal security and its external aspects to help build the capacity of law enforcement officials while seeking to avoid duplication of efforts and achieve better coordination.

Joint training initiatives, e.g. the integrated initial training for law enforcement agencies of the French Gendarmerie and the Spanish Guardia Civil, should be promoted. Appropriate EU funding through relevant instruments such as Erasmus+ should be addressed.

Furthermore, there is a growing need to manage efficiently the expertise of specialists in EU law enforcement agencies. In this area, the added value of expert law enforcement networks is essential to foster mutual knowledge and exchange. The output of best-practices and guidance

based on operational experience should be maximised, through the elaboration of relevant training material and the execution of training activities, with the support of EU institutions through CEPOL.

8. Integrated approach to security - internal and external security nexus and hybrid threats

Europe's internal and external security are inherently linked: a more joined up approach between Member States and EU institutions, and between the internal and external dimensions of EU's policies is necessary. This is particularly relevant to the implementation of the Sustainable Development Goals, migration and security issues. Instability in conflict areas and post-conflict areas outside Europe contributes to conditions conducive to the spread of terrorism, uncontrolled migration and cross-border crime. Moreover, non-EU actors may take advantage of criminal organisations active within the Union to further their own agendas. It is essential to address the threats coming from those countries potentially having an impact on the internal security of the EU, also in coordination with the EU Common Security and Defence Policy (CSDP). Cooperation between justice and home affairs actors and civilian crisis management structures and missions is an integral part of the Civilian CSDP Compact[9], agreed in November 2018 to enhance civilian crisis management.

The EU currently has civilian crisis management missions in regions such as the Sahel, the Horn of Africa and Iraq, all considered as critical in terms of the internal security of Europe. The functioning of such missions should enable us to curb the spread of serious and organized international crime, terrorism and uncontrolled migration more efficiently and to prevent them from turning into threats for the EU. We should encourage new opportunities for cooperation between JHA Agencies, Member States' authorities and the CSDP missions. Ongoing coordination with CSDP missions should be carried out from strategic planning, via operational planning, to implementation, as JHA Agencies and CSDP missions often target similar security challenges and draw upon a limited set of Member State resources.

The Regulation on the European Border and Coast Guard, will introduce significant changes into the role of the European Border and Coast Guard Agency (Frontex) in third countries. The Agency will now be able to resort to a strong standing corps that is operational and deployable anywhere in the world to back up integrated border security in Europe. Other EU Agencies from the area of Justice and Home Affairs, such as Europol, Cepol, Eurojust and the EU Drugs Agency (EMCDDA), should also continue their targeted engagement in the external dimension of our security policies in a coordinated manner, in line with their respective mandates, and taking into account their capacities.

Internal security actors play a key role in preventing and countering hybrid threats. Their work has the potential to bolster the resilience of society and to build up resistance against various types of attempts to hybrid influence. Through effective communication, public authorities can ward off disinformation and election interference, and help narrow down the room for manoeuvre of actors whose toolkits include hybrid threats. This dimension is particularly important in incidents directly or indirectly affecting the general public, such as terrorist attacks, violent crime, other

[9] https://www.consilium.europa.eu/media/37027/st14305-en18.pdf

serious crime and disasters. Because of their physical presence in the streets, at border-crossing points, in seaports, on main roads, at airports and in many other key locations, law enforcement authorities are in the vanguard and therefore play a key role in identifying threats first-hand. EU agencies also play an important role in identifying, preventing and addressing these threats.

The ongoing debate on how to counter hybrid threats has focused increasingly on the protection of critical infrastructures. While the Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (2008/114/EC) succeeded in drawing attention to the importance of protecting such infrastructures, it failed to address their strong interdependencies and the threat that cyber and hybrid attacks may pose to their functioning. The implementation of the Directive is currently being evaluated.

9. Operational cooperation between law enforcement authorities: thematic discussion

Differences in national legislation, decision-making processes and operating models represent a challenge to operational cooperation. In individual cases, cooperation is also hampered by discrepancies in national data collection and processing practices, resulting from differences between individual Member States in terms of administrative systems, technical solutions and functional arrangements. When dealing with an urgent case, national entities may not even be aware of the range of operational alternatives and information exchange channels available.

Cross-border operational cooperation between law enforcement authorities draws on cooperation at different levels under instruments such as the Prüm decision[10] and the Schengen acquis on operational cooperation (essentially the 1985 Convention Implementing the Schengen Agreement – CISA). Council non-binding guidelines, e.g. best practices guidelines for PCCCs adopted in 2008 and revised in 2011, also exist. However, due to the broad nature of the above instruments, the Member States have regulated the practical arrangements of their cooperation by signing agreements facilitating bilateral and multilateral operational actions. While this can mean a much deeper regional cooperation than the one foreseen in the Prüm Decision or the Schengen acquis on operational cooperation in some geographical areas, it can also bring about fragmentation, and the extent of law enforcement operational cooperation now varies greatly between Member States.

Similar discrepancies can be seen in the availability of communication tools and other technical aids that are not always compatible and in language skills and training. It also appears that operational cooperation tends to be reactive, rather than proactive and based on risk assessments and analysis. Operational cooperation between law enforcement authorities should be intensified by developing and using new ways of working together and exchanging information, while relying on new technological applications and tools. These could include drones, automatic number plate recognition technologies, single-search interfaces for available databases or push-to-talk applications operating based on mobile data networks rather than state-specific radio frequencies that hamper cross-border policing.

[10] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

More should also be done to systematically strengthen and enrich the overall analysis of the operating environment for law enforcement authorities[11]. The working methods of the different law enforcement authorities of the Member States could then be developed proactively, taking into account the challenges arising from their operating environment, including a better interaction with other internal security actors, as well as other policy areas with impact on security, e.g. internal market developments and environment. This can also facilitate standardised technical solutions or targeted capacity building and training for law enforcement, as well as proactive operations at local/regional level.

A main platform for operational cooperation is the EU Policy Cycle for serious and organised international crime[12], including its operational platform, EMPACT. As a working tool based on threat analysis and risk assessments, EMPACT has proven to be a well-functioning model for aligning the operational activities of law enforcement authorities across the Union to combat and prevent serious and organised crime. However, the effectiveness of the Policy Cycle must be further intensified and enhanced in terms of its criminal intelligence-based nature, more accessible financing mechanisms, cooperation with third countries and better use of information received from other actors, including the private sector.

Another challenge involves identifying and removing the obstacles to operational cooperation between law enforcement authorities, such as incompatible radio frequencies in border areas or the necessity to supplement existing legal bases by more detailed bilateral agreements.

[11] Analyses and situation updates on the operating environment also require reliable crime statistics, which can be obtained, for example, by using and upgrading Eurostat statistics (see Eurostat, 2018: Sustainable development in the European Union, pp. 297–311 (homicide rates, perceptions of crime)).
[12] Document 15358/10