Council of the European Union

**Brussels, 28 July 2017
(OR. en)**

11550/17

**DAPIX 278
COSI 175
FREMP 88
CT 78
FRONT 344
COPEN 249
JAIEX 54
ENFOPOL 378
CYBER 118
JAI 725**

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	27 July 2017
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2017) 407 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Ninth progress report towards an effective and genuine Security Union

Delegations will find attached document COM(2017) 407 final.

Encl.: COM(2017) 407 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL

Ninth progress report towards an effective and genuine Security Union

{SWD(2017) 278 final}

EN

EN

I. INTRODUCTION

This is the ninth monthly report on the progress made towards building an effective and genuine Security Union and covers developments under two main pillars: tackling terrorism and organised crime and the means that support them; and strengthening our defences and building resilience against those threats.

This report sets out the conclusions the Commission draws from the **comprehensive assessment of the Union's action in the area of internal security** published together with this report.[1] Launched in December 2016, the assessment scrutinised the relevance and effectiveness of EU policies and instruments to support Member States in tackling terrorism and preventing radicalisation, disrupting organised crime and fighting cybercrime. Looking at action taken at EU level in the area of internal security, the assessment is based on in-house analysis by the Commission services, surveys carried out with Member States' authorities and EU agencies, and an inclusive dialogue with a wide range of stakeholders including the European Parliament, national Parliaments, civil society, think tanks, academia and industry representatives.

While the **overall result of the comprehensive assessment is positive** and confirms the appreciation and relevance of the main instruments of EU security policy, the assessment also identified **challenges and gaps** that have an impact on effective cooperation in the Security Union. This report sets out how the Commission sees the way to address these challenges and gaps with the aim further to increase the effectiveness of EU security policy. This includes the need further to develop and adjust existing policies and tools to respond to the evolving threat posed by terrorism, as also highlighted by the European Council conclusions[2] of 22-23 June 2017, the G20 Action Plan on Countering Terrorism[3] of 7 July 2017 and the Taormina G7 Summit statement[4] on the fight against terrorism and violent extremism of 26 May 2017.

This report also provides an update on progress made in the implementation of priority files on security, with the next steps taken to **prevent terrorist financing** through trafficking in cultural goods and to enhance the **exchange of information** through the interoperability of information systems and their full implementation. In terms of non-legislative action, this report provides an update on measures taken to **prevent radicalisation online**, strengthen the **protection of soft targets** and support national action through **EU funding** for internal security policies. Finally, this report also addresses recent developments on the external dimension that are relevant for the work towards an effective and genuine Security Union.

II. COMPREHENSIVE ASSESSMENT OF EU SECURITY POLICY

1. Overall assessment: EU action brings added value in supporting Member States

The comprehensive assessment shows that stakeholders consider the Union's action in the area of internal security and the instruments used as **appropriate, relevant and effective** in producing positive results. EU policies on internal security are perceived as bringing added value in supporting Member States' action, in line with Member States' operational responsibility for ensuring security and the supporting role entrusted to EU institutions and

---

[1] SWD(2017) 278 final (26.7.2017).
[2] http://www.consilium.europa.eu/en/meetings/european-council/2017/06/22-23-euco-conclusions_pdf/.
[3] http://www.consilium.europa.eu/press-releases-pdf/2017/7/47244662401_en.pdf.
[4] http://www.consilium.europa.eu/en/press/press-releases/2017/05/26-statement-fight-against-terrorism/.

2

EU agencies by the Treaties. Neither substantial negative side effects, nor significant duplication or overlap were identified.

Notably, the comprehensive assessment highlights the added value of EU action in facilitating **information exchange and operational cooperation**. Instruments and tools such as the Schengen Information System, joint investigation teams, the European Arrest Warrant or mutual legal assistance support national authorities in collecting and exchanging information and evidence, allow them to carry out coordinated operational action, and help them bring offenders to justice. In addition, the overall assessment is that EU measures have contributed to improve national capabilities to counter terrorism, serious and organised crime and cybercrime, including through training, exchange of best practices and cross-border cooperation. Frameworks for cooperation, such as the EU Policy Cycle for organised and serious international crime, help define common priorities for operational action by Member States' authorities at national level and across borders. EU agencies in the area of justice and home affairs have turned into central actors in their respective areas of competence, as illustrated by the support provided by Europol through its specialised centres[5] or Eurojust's role in facilitating the implementation of the European Arrest Warrant and the European Investigation Order.

In terms of **EU legislation**, the comprehensive assessment shows that overall, stakeholders are satisfied with the EU framework in the area of internal security and the legal certainty it brings. EU legal framework for internal security policy has developed over time and has proven able to adjust to evolving threats. While no major gaps in legislation have been identified, the comprehensive assessment indicates a need for targeted changes and additions to the EU framework in order to address evolving threats or to streamline existing rules to reduce complexity for those who apply them on the ground (see Section II.2 below, including on the Commission's conclusions from these findings).

The comprehensive assessment confirms that the compliance with **fundamental rights** is a key characteristic of EU security policy, in line with the legal obligation under the Treaties. In addition to effective judicial control by the Court of Justice of the European Union, the Commission has developed several mechanisms to mainstream fundamental rights in the formulation of legislative and policy proposals. This includes assessing the impact of planned policy measures on fundamental rights as part of impact assessments under better regulation[6], or involving the European Data Protection Supervisor and the EU Fundamental Rights Agency at an early stage of working on specific initiatives. The on-going work on the interoperability of information systems is one example where the input and guidance of the European Data Protection Supervisor and the EU Fundamental Rights Agency is taken into account at an early stage of developing a new policy approach.[7] Fundamental rights are also taken into consideration when evaluating the impact and effectiveness of EU instruments and policies to verify whether they remain necessary, proportionate and fit for purpose. The Commission also assists national authorities to ensure compliance with fundamental rights in implementing relevant EU legislation. The Commission will continue to apply and further develop these mechanisms to ensure full compliance with fundamental rights in EU security

---

[5]   The European Counter Terrorism Centre (ECTC), the European Cybercrime Centre (EC3) and the European Migrant Smuggling Centre (EMSC).

[6]   See the Commission Staff Working Paper on Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments (SEC(2011) 567 final, 6.5.2011).

[7]   See the Seventh progress report towards an effective and genuine Security Union (COM(2017) 261 final, 16.5.2017).

policy, in line with the understanding that protecting citizens' security and complying with fundamental rights are complementary.

2. Main challenges for an effective EU security policy and how to address them

While the overall conclusion of the comprehensive assessment is positive, the assessment also identified challenges and gaps that have an adverse effect on cooperation in the Security Union. These challenges and gaps can be summarised as follows:

- the **incomplete implementation** of some EU policies and instruments at national level reduce their effectiveness;
- the **complexity** of some EU instruments and tools make it harder for national authorities to use them to full effect;
- limited **capacities** at national level call for further pooling of resources and expertise at EU level and synergies across policy areas;
- **evolving threats** which require the EU to update its instruments and tools.

By identifying these challenges and gaps, the comprehensive assessment confirms a number of policy initiatives the Commission has recently launched and calls for further action.The Commission will follow up on these findings in accordance with better regulation principles.

Supporting the full implementation of EU measures

The comprehensive assessment shows that for a number of key EU policies and instruments in the area of internal security, there is a **lack of full implementation** by Member States at national level. Examples for this are the legislation in the area of organised crime[8] or the Prüm framework[9] for the exchange of DNA data, fingerprint data and vehicle registration data. Lack of full implementation of these instruments impedes their effectiveness and prevents all Member States from exploiting their full potential.

The Commission will continue to **support Member States in implementing EU legislation** during the transposition period. An example for this is the support for the implementation of the EU Passenger Name Record (PNR) Directive[10] that needs to be implemented by 25 May 2018. The Commission presented an implementation plan[11], provided additional funding and organises regular meetings with Member States experts to share related knowledge, expertise and best practice (see Section III.1 below). Another example is the on-going implementation of the Directive on security of network and information systems (NIS Directive) that needs to be implemented by 9 May 2018.[12] In line with the findings of the comprehensive assessment, the Commission will pay special attention to the implementation of the Directive on combating terrorism[13] and recent legislation on terrorist financing[14], as the comprehensive assessment reveals that some stakeholders highlighted the risk of difficulties in implementing these instruments.

---

[8]   Notably the Framework Decision on the fight against organised crime (Council Framework Decision 2008/841/JHA, 24.10. 2008).
[9]   Council Decisions 2008/615/JHA and 2008/616/JHA (23.6.2008).
[10] Directive (EU) 2016/681 (27.4.2016).
[11] SWD(2016) 426 final (28.11.2016).
[12] Directive (EU) 2016/1148 (6.7.2016).
[13] Directive (EU) 2017/541 (15.3.2017).
[14] Directive (EU) 2015/849 (20.5.2015).

The Commission will also continue to exercise its role as Guardian of the Treaties and commence infringement proceedings whenever necessary to ensure the full application of EU law in the area of internal security. In line with the findings of the comprehensive assessment, the Commission will continue to combine the use of these **enforcement powers** with measures to share knowledge and expertise with the Member States concerned. An example of this is the technical support provided by the Commission in parallel to the infringement proceedings against those few Member States that have not yet implemented the Prüm framework (see Section III.1 below).

Member States' authorities referred to the lack of technical expertise and financial resources as important reasons for delays in the implementation process, especially in cases of new or upgraded information. The Commission notes that **EU funding** is available under the Internal Security Fund – Police, but the absorption by Member States should be improved, with an implementation rate of 26% on 15 June 2017 (see also Section III.2 below). The Commission will continue to support Member States in using the available funding to best effect.

Reducing the complexity of EU instruments and tools

The comprehensive assessment indicates that for some EU instruments, the **complexity of the EU legislation** governing these tools impedes their effective use by national authorities. An example of this is the set of diverging EU rules on access to EU information systems by law enforcement authorities or the current legal frameworks for obtaining cross-border access to electronic evidence that reflect traditional concepts of territoriality and are challenged by the cross-jurisdictional nature of electronic services and data flows. This is partially because the different instruments were developed over a longer period of time, which in some cases has resulted in a complex web of instruments that makes it difficult for national authorities to use these tools. Moreover, EU legislation has not always brought the necessary clarity in terms of definitions, resulting in diverging rules in Member States that hamper operational cooperation. This was notably the case in the area of counter-terrorism prior to the adoption of the Directive on combating terrorism[15] that criminalises acts such as the financing of terrorism, undertaking training or travelling for terrorist purposes, as well as organising or facilitating such travel.

The Commission has already taken action to address the complexity of EU legislation highlighted by the comprehensive assessment. In the area of information exchange, the Commission identified the complex landscape of differently governed information systems as an obstacle that impedes the work of national authorities,[16] and it proposed a way forward to overcome this obstacle through the interoperability of information systems[17], including with more streamlined rules for law enforcement access respecting fundamental rights, in particular data protection. The Commission also reviewed the mechanisms for obtaining cross-border access to electronic evidence. On that basis, the Commission implements practical measures to improve such access within the current legislative framework while working on an impact assessment to inform possible future legislative action.[18]

---

[15] Directive (EU) 2017/541 (15.3.2017).
[16] See the Communication on Stronger and Smarter Information Systems for Borders and Security (COM(2016) 205 final, 6.4.2016).
[17] See the Seventh progress report towards an effective and genuine Security Union (COM(2017) 261 final, 16.5.2017).
[18] See the Eighth progress report towards an effective and genuine Security Union (COM(2017) 354 final, 29.6.2017).

The Commission will also **review the legislative acts identified by the comprehensive assessment** as possibly obsolete or outdated. In November 2014, the Commission proposed to repeal 24 acts in the area of police cooperation and judicial cooperation in criminal matters.[19] The co-legislators adopted the proposals on 20 January 2016 and in all 26 acts were repealed.[20]

The comprehensive assessment also shows the importance of **training** to increase end-users' knowledge of existing EU instruments and their ability to use them effectively. Stakeholders also referred to the added value of exchange and secondment programmes for national officials as a way to share best practice in the use of EU instruments. The Commission works closely with the European Union Agency for Law Enforcement Training (CEPOL) to ensure that its training programme is in line with Union priorities in the area of security and that the Agency contributes to equipping national officials with the knowledge and skills they need to cooperate effectively with their counterparts in other Member States, making full use of the agencies' new mandate from 1 July 2016.[21] The Commission supports a range of training programmes developed by the European Judicial Training Network (EJTN) for prosecutors and judges implementing Union legislation on judicial cooperation in criminal matters.

Capacity building at EU level through pooling of resources and expertise and exploiting synergies

It results from the comprehensive assessment that there is scope for further pooling of resources at EU level. Where individual Member States lack specific expertise or resources, there is potential benefit in the development of **shared capacity at EU level**. Stakeholders referred in particular to technology-intensive areas such as cybersecurity, chemical, biological, radiological or nuclear (CBRN) materials or the analysis of big data or open sources. **EU agencies** play a central role in providing shared resources to individual Member States. For example, the European Cybercrime Centre (EC3) at Europol supports national authorities in the fight against cybercrime and the law enforcement response to large-scale cyber-attacks, through forensic expertise or with cybercrime-related information from public, private and open sources. The European Counter-Terrorism Centre and the European Migrant Smuggling Centre at Europol perform similar support functions in their respective areas. Another example is the role played by the EU Agency for Network and Information Security (ENISA) in supporting the cooperation between Member States under the Directive on security of network and information systems (NIS Directive). The comprehensive assessment shows that the support provided by EU agencies is considered highly valuable by stakeholders. The Commission has worked to ensure that the EU agencies have the means they need to fulfil this support function.

Networks at EU level are another way of pooling expertise in specific areas of internal security. The comprehensive assessment underlines the added value of European networks or cooperation structures that complement the work of EU agencies and foster operational cooperation. This includes networks specialised in environmental crime (EnviCrimeNet), drug trafficking (Maritime Analysis and Operations Centre – Narcotics), crime prevention (European Crime Prevention Network), special intervention units (ATLAS Network), chemical, biological, radiological or nuclear (CBRN) materials (CBRN Advisory Group) or

---

[19] COM(2014) 713 final, COM(2014) 714 final and COM(2014) 715 final (28.11.2014). These proposals were based on an assessment of the legal acts related to the Area of Freedom, Security and Justice that was carried out in the light of the end of transitional provisions set out in the Protocol 36 to the Treaty of Lisbon.

[20] Regulation (EU) 2016/93, Regulation (EU) 2016/94 and Regulation (EU) 2016/95 (20.1.2016).

[21] Regulation (EU) 2015/2219 (25.11.2015).

transport security (Airpol and Railpol). The Commission will continue using this network approach where necessary, as is the case with the recently established EU Soft Target Protection Policy Group to allow for a more structural exchange of information and sharing of best practice on operational action to protect soft targets.

It results from the comprehensive assessment that due to the cross-cutting nature of the challenges related to terrorism, serious crime and cybercrime, there is scope for further exploiting **synergies at EU level between security policy and related policy areas**. Examples include the need for closer cooperation between police authorities, border guards and customs authorities, or the links between security policy and transport police in areas such as aviation security or maritime security. The Commission responded to this need for cross-sectorial action with the creation of a specific Commissioner portfolio for the Security Union assisted by a cross-cutting Task Force drawing on the expertise of the entire Commission.

The comprehensive assessment also highlights that the EU level provides added value to national authorities by **bringing together various actors** from outside the public sector. Stakeholders refer to the importance of cooperation between public authorities and industry on tackling cybercrime or radicalisation online, or the importance of involving local practitioners, academics and researchers in efforts to prevent violent radicalisation in communities. The Commission will continue to support this work with entities such as the EU Internet Forum or the Radicalisation Awareness Network Centre of Excellence. The Commission will also consider organising regular strategic dialogues on security policy with a wide range of stakeholders.

Addressing evolving threats

An overall challenge for EU security policy is the need to ensure that instruments and tools are up-to-date to address evolving security threats. The comprehensive assessment shows that new and emerging threats have repeatedly required targeted revision of existing EU tools or legislation on internal security. In the area of counter-terrorism, the overall conceptual framework for EU action on internal security has remained valid and allowed adapting individual instruments and tools in response to a rapidly changing security environment.

The Commission will continue to assess the need for targeted changes to existing instruments and tools on internal security. Recent examples include the setting up of a High-Level Expert Group on Radicalisation[22] to facilitate the further development of EU policies in response to an unprecedented scale of radicalisation and the upcoming review of the 2013 Cybersecurity Strategy to provide an up to date and effective response to the growing threat of cybercrime.

The upcoming **European Parliament special committee on terrorism**[23] provides an additional opportunity further to analyse if the existing EU counter-terrorism measures are appropriate to respond to the evolving terrorist threat in Europe, and to identify practical and legal obstacles that need to be addressed. The Commission will actively contribute to the work of the special committee, seeking to achieve an outcome that will provide a basis for further joint action with the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) and the Council.

---

[22] See the Eighth progress report towards an effective and genuine Security Union (COM(2017) 354 final, 29.6.2017).

[23] http://www.europarl.europa.eu/news/en/press-room/20170629IPR78658/special-committee-to-tackle-deficiencies-in-the-fight-against-terrorism.

III.   IMPLEMENTATION OF PRIORITY FILES ON SECURITY

1. Legislative initiatives

On 13 July 2017, the Commission adopted a proposal[24] for a Regulation to **prevent the import and storage in the EU of cultural goods illicitly exported from a third country**, thereby reducing trafficking in cultural goods, combatting terrorism financing and protecting cultural heritage. This is a further step in implementing the February 2016 Action Plan to step up the fight against the financing of terrorism[25], and it also responds to the call by the Security Council of the United Nations[26] to take steps to counter the illicit trade and trafficking in cultural property in particular when originating from a context of armed conflict and conducted by or benefiting to terrorist groups. Once adopted by the co-legislators, the Commission proposal will establish a common definition for cultural goods at import, ensure importers exercise diligence when buying cultural goods from third countries, determine standardised information to certify the goods are legal, and provide for effective deterrents to trafficking. The Commission calls on the co-legislators to work on the proposal as a matter of priority.

There is also further progress in the work on stronger and smarter information systems for borders and security. On 12 July 2017, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) and the Council' Committee of the Permanent Representatives (COREPER) confirmed the agreement reached on the **Entry/Exit System** (EES). Proposed by the Commission in April 2016,[27] the system will register entry and exit data of non-EU nationals crossing the EU's external borders and therefore contribute to enhancing external border management and internal security. The political agreement on the Entry/Exit System is an important step towards achieving full interoperability of EU information systems by 2020, in line with the Commission's new approach to the management of data for borders and security.[28] At the informal meeting of the Justice and Home Affairs Council in Tallinn on 6/7 July 2017, Member States reiterated their commitment to work on the interoperability of information systems as a matter of priority. The Commission calls on the co-legislators to accelerate the work on related legislative proposals on information systems that are currently under discussion.[29]

Work also continues on implementing existing systems and maximising their benefits – another key area for action to make the information systems for borders and security stronger and smarter. As part of the support provided to the implementation of the **Passenger Name Records (PNR) Directive**, the Commission services held on 22 June 2017 a fifth meeting with Member States experts to share related knowledge, expertise and best practice. As less

---

[24]   COM(2017) 375 final (13.7.2017).

[25]   COM(2016) 50 final (2.2.2016). See the Eighths progress towards an effective and genuine Security Union (COM(2017) 354 final, 29.6.2017) for an overview of the state of play of implementation of the Action Plan.

[26]   UN Security Council Resolution 2347 (24.3.2017).

[27]   COM(2016) 194 final (6.4.2016).

[28]   See the Seventh progress report towards an effective and genuine Security Union (COM(2017) 261 final, 16.5.2017).

[29]   These are the proposal to establish a European Travel Information and Authorisation system (ETIAS) (COM(2016) 731 final, 16.11.2016), the proposals to strengthen the Schengen Information System (COM(2016) 881 final, 882 final and 883 final, 21.12.2016), the proposal to Eurodac (COM(2016) 272 final, 4.5.2016) and the supplementary proposal to facilitate the exchange of criminal records of third-country nationals in the EU through the European Criminal Records Information System (ECRIS) (COM(2017) 344 final, 29.6.2017).

than one year is left before the transposition deadline (25 May 2018), the Commission once again encouraged Member States to strengthen their efforts to ensure the timely establishment of a functional PNR system as an important instrument in the response to the threat of terrorism. The Commission sent letters to those Member States that appear to be less advanced in the implementation process in order to address the possible obstacles they might face and assess whether additional support is possible, including bilateral support offered by a number of those Member States that are at an advanced stage of implementing the PNR Directive.

While some Member States have made progress in the implementation of the **Prüm Decisions**[30], the Commission has had to use its infringement powers to ensure full implementation. To that end, the Commission sent Reasoned Opinions to Croatia, Ireland and Italy on 18 May 2017. In addition to using its powers under the Treaties, the Commission continues to support Member States by providing funding for implementation under the national programmes within the Internal Security Fund – Police. The Commission will provide an additional EUR 22 million to these national programmes for 2017 and this funding can be used for the implementation of Prüm.

On 7 July 2017, Ministers of Justice discussed the Commission's proposal on **mutual recognition of freezing and confiscation orders**[31] in the Informal Justice and Home Affairs Council meeting held in Tallinn. The Commission calls on the co-legislators to progress swiftly on this proposal in order to improve the recovery of criminal assets in cross-border cases.

2. Implementation of non-legislative actions

Countering radicalisation online remains a priority in the fight against terrorism, and the Commission is accelerating its work to support Member States in addressing this challenge. Following a meeting of the EU Internet Forum[32] at senior officials level on 27 June 2017, the members of the EU Internet Forum set out on 17 July 2017 an **Action Plan to combat terrorist content online**. This includes measures to step up the automated detection of illegal terrorist content online, share related technology and tools with smaller companies, achieve the full implementation and use of the 'database of hashes', and empower civil society on alternative narratives. Given the urgency of the matter, the Commission services will convene another meeting of the EU Internet Forum at senior official level in September and will report on progress made in the implementation of the Action Plan in one of the forthcoming Security Union progress report.

Recent terrorist attacks have once again turned the focus on the need to strengthen the **protection of soft targets**, calling for innovative responses to protect crowded places. On 30/31 May 2017, the Commission services hosted a workshop with experts from Member States and third countries to exchange good practices and lessons learned on soft target

---

[30] These Council Decisions (Council Decisions 2008/615/JHA and 2008/616/JHA, 23.6.2008) have a particular focus on combating terrorism and cross-border crime. They introduced rules and procedures to allow Member States to quickly search each other's DNA analysis files, fingerprint identification systems and vehicle registration databases. The Council Decisions should have been implemented fully by Member States by August 2011.

[31] COM(2016) 819 final (21.12.2016).

[32] The Commission has been working over the last two years with key internet platforms, Member States and other stakeholders under the EU Internet Forum to ensure the voluntary removal of online terrorist content and support civil society in the dissemination of alternative narratives.

protection. This workshop, organised in the framework of the Global Counterterrorism Forum, complemented the efforts launched in February 2017 to develop an EU policy and practitioner platform to enhance EU resilience against soft target attacks Moreover, as a practical measure supported by the Commission, Belgian and Dutch Police special intervention forces conducted on 29 June 2017 a cross-border soft target exercise involving a simulation of synchronised terrorist attacks on public schools. Involving police forces, first responders and state emergency response teams, this exercise aimed to measure preparedness and crisis management functions in case of attacks taking place simultaneously in neighbouring countries. The Commission services will organise a special de-briefing for all Member states to disseminate best practices learned from this exercise.

EU funding is an important tool to support Member States in implementing the steps needed to build an effective and genuine Security Union. Given the evolving threat posed by terrorist, organised crime and cybercrime, the Commission will provide **EUR 90 million in 2017 to support Union actions** under the Internal Security Fund – Police[33], doubling the amount provided in 2016. The respective annual work programme[34], setting out funding priorities for targeted cross-border actions in the area of internal security, intends to support Member States' efforts to counter terrorism through projects to prevent terrorist financing, counter radicalisation, support civil society in the dissemination of alternative narratives and strengthen the protection of critical infrastructure. The Commission intends to also provide funding for cross-border projects to tackle priority crime threats such as trafficking in human beings, drugs trafficking, firearms trafficking and environmental crime.[35]

For the first time under the Internal Security Fund – Police, the annual work programme 2017 intends to provide funding for projects tackling cybercrime. This reflects the evolving cyber threat, as witnessed by recent cyber-attacks, and the fact that for almost all types of organised crime, criminals are deploying technology with ever-greater skill and to ever-greater effect. To strengthen the exchange of information, the Commission intends to provide funding for projects that seek to maximise the benefits of existing EU information systems. This is a priority in the work on stronger and smarter information systems for borders and security[36], and it will support the efforts to make EU information systems interoperable.[37] Finally, the Commission intends to provide funding to reinforce cross-border police cooperation, in line with its May 2017 recommendation on proportionate police checks and police cooperation in the Schengen area.[38]

This funding comes on top of the support provided to Member States through their national programmes under the Internal Security Fund - Police. For the period **from 2014 to 2020, the Commission provides a total of EUR 754 million to 26 Member States** for measures to fight crime and manage risk and crisis.[39] This funding can be used for a wide range of initiatives to ensure a high level of security in the EU, such as setting up information systems,

---

[33] Regulation (EU) No 513/2014 (16.4.2014).
[34] The Commission intends to adopt the annual work programme for 2017 for Union actions within the framework of the Internal Security Fund – Police in September 2017.
[35] See the crime threat priorities set out in the Sixth progress report towards an effective and genuine Security Union (COM(2017) 213 final, 12.4.2017).
[36] COM(2016) 205 final (6.4.2016).
[37] See the Commission's new approach to the management of data for borders and security as set out in the Seventh progress report towards an effective and genuine Security Union (COM(2017) 261 final, 16.5.2017).
[38] C(2017) 3349 final (12.5.2017).
[39] All Member States except Denmark and the United Kingdom participate in the implementation of the Internal Security Fund – Police.

acquisition of operational equipment, promoting training schemes and ensuring operational cooperation. However, there is clear room for improvement in the way Member States absorb this funding. The Commission therefore calls on Member States to make full use of this funding to implement the priorities in the Security Union.

3. External dimension

The Leaders of the G20 adopted at the summit in Hamburg on 7/8 July 2017 the **Action Plan on Countering Terrorism**. By calling for action to address the evolving threat of returning foreign terrorist fighters, facilitate the exchange of information, fight terrorism finance and countering radicalisation and the use of internet for terrorist purposes, the Action Plan confirms the current priorities of EU action in the Security Union. The Commission and the European External Action Service will continue to work closely with its partners outside the EU in implementing these policies.

On 26 July 2017, the Court of Justice of the European Union delivered its opinion on the compatibility of the **agreement between the EU and Canada on the transfer and processing of passenger name record (PNR) data** with the Treaties.[40] The agreement was signed in 2014 and the Council requested the European Parliament to approve it. The European Parliament decided to refer the matter to the Court of Justice in order to ascertain whether the agreement envisaged was compatible with EU law guaranteeing the respect for private and family life and the protection of personal data. The Commission will revert to this issue in the next Security Union progress report in September 2017.

The **informal meeting of the EU-Eastern Partnership Ministers of Justice and Home Affairs** in Tallinn on 7 July focused on the fight against cybercrime, the fight against corruption, and essential judicial reforms. Minister reiterated their joint commitment to take further action to combat cybercrime and strengthen cybersecurity. They discussed legislative and operational challenges in the fight against cybercrime, with the perspective of enhancing cooperation at both regional and international levels and pursuing further action in the framework of the Eastern Partnership rule of law panel.

On 19 June 2017, the Foreign Affairs Council adopted conclusions on the **external aspects of maritime security** that highlight the role of the EU as a global maritime security provider and call for enhanced information sharing, exchange of good practices, increased coordination of EU initiatives and international cooperation at sea to confront the emerging challenges and threats at sea.

On 17 July 2017, the Foreign Affairs Council discussed priorities for the implementation of the **EU Global Strategy for Foreign and Security Policy** in 2017-2018. Ministers highlighted the need to strengthen further the link between the internal and external dimension on security, counterterrorism and countering hybrid threats. Ministers also agreed on two additional tracks for further work on global governance and regional cooperation, including on strengthening maritime security and enhancing the cyber security of the Union.

On 19 July 2017, the Commission and the EU High Representative presented a report[41] taking stock of the progress made in implementing the April 2016 **Joint Framework on**

---

[40]   https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf.
[41]   JOIN (2017) 30 final (19.7.2017).

Countering Hybrid Threats.[42] It reports progress on 22 actions to raising awareness on hybrid threats, build resilience against these threats and step up cooperation between the EU and NATO.

In the context of the **EU-NATO** strategic partnership and cooperation, the Foreign Affairs Council on 19 June 2017 adopted conclusions on the progress made in implementing the common set of proposals (42 actions) endorsed by EU and NATO Ministers on 6 December 2016. The progress report underlines the need for cooperation between the two organisations in the current strategic environment where the EU and NATO are both faced with unprecedented challenges, and neither organisation has the full range of tools to address these security challenges on its own. The report shows that the activities of the two organisations are complementary to each other and help to achieve a common goal. The newly created European Centre of Excellence for Countering Hybrid Threats in Helsinki, and the establishment of the EU Hybrid Fusion Cell and its interaction with the newly created NATO Hybrid Analysis Branch, further strengthen cooperation between the EU and NATO.

IV.   CONCLUSION

This report focuses on the conclusions the Commission draws from the comprehensive assessment of the Union's action in the area of internal security published together with this report. While the overall result of the comprehensive assessment is positive and confirms the relevance and effectiveness of the Union's action in the area of internal security, the Commission will continue to take action to address the obstacles and gaps identified by: (1) supporting the full implementation of EU measures, (2) reducing the complexity of EU instruments and tools, (3) building further capacity at EU level through the pooling of resources, and (4) addressing evolving threats. The Commission will present the comprehensive assessment to the European Parliament and the Council, and it encourages the two Institutions to engage in a dialogue to examine its findings.

The next Security Union progress report will be presented in September 2017.

---

[42]   JOIN (2018)18 final (6.4.2016).