Council of the European Union

Brussels, 20 October 2017
(OR. en)

13478/17

CT 109
COSI 238
MI 738
COPEN 311
JAIEX 81
ENFOPOL 473
CYBER 156
EF 240
SIRIS 172
DAPIX 336
DATAPROTECT 162
PROCIV 86
JAI 942

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	18 October 2017
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2017) 608 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Eleventh progress report towards an effective and genuine Security Union

Delegations will find attached document COM(2017) 608 final.

Encl.: COM(2017) 608 final

EUROPEAN
COMMISSION

Brussels, 18.10.2017
COM(2017) 608 final

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

Eleventh progress report towards an effective and genuine Security Union

I. INTRODUCTION

This is the eleventh 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.

President Juncker underlined in the State of the Union address[1] that the European Union must be stronger in fighting terrorism, building on the real progress made in the past three years. As announced in the letter of intent[2] to the European Parliament and the Council Presidency and the accompanying Roadmap for a More United, Stronger and More Democratic Union, in this report the Commission sets out a **package of anti-terrorism measures** to be undertaken over the next sixteen months. These operational measures will help Member States address significant vulnerabilities exposed by recent terrorist attacks and will make a real difference in enhancing security. This will contribute to completing a Security Union where terrorists can no longer exploit loopholes to commit their atrocities. Beyond these practical measures for the short term, the Commission is working towards a future European Intelligence Unit, as announced by President Juncker as part of his vision for the European Union by 2025.

The anti-terrorism package includes:

- measures to support Member States in **protecting public spaces** (chapter II), including an Action Plan to support the protection of public spaces and an Action Plan to enhance the preparedness against chemical, biological, radiological and nuclear security risks;
- measures to **cut off access to the means used by terrorists** to prepare and carry out attacks such as **dangerous substances** or **terrorist financing** (chapter III), including a Recommendation on immediate steps to prevent misuse of explosives precursors, as well as measures to support law enforcement and judicial authorities when they encounter the **use of encryption** in criminal investigations;
- the next steps on **countering radicalisation** (chapter IV);
- the next steps on strengthening the **external dimension** of counter-terrorism (chapter V), including proposals for Council Decisions on the conclusion, on behalf of the EU, of the Council of Europe Convention and Additional Protocol on the Prevention of Terrorism as well as a Recommendation to the Council to authorise the opening of negotiations for a revised passenger name record agreement with Canada.

[1] http://europa.eu/rapid/press-release_SPEECH-17-3165_en.htm.
[2] https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_en.pdf.

II. MEASURES TO IMPROVE PROTECTION AND RESILIENCE AGAINST TERRORISM

1. Enhanced protection of public spaces

In propaganda and in the choice of targets, the terrorists' focus is shifting to public spaces such as pedestrian precincts, tourist sites, transport hubs, shopping malls, concert halls and city squares, as seen in attacks in, for example, Barcelona, Berlin, Brussels, London, Manchester, Nice, Paris and Stockholm. What all these so-called "soft targets" have in common is their open nature and public character, as well as the high concentration of people, which makes them intrinsically vulnerable.

We can do more to reduce the vulnerabilities of these locations, detect threats at an earlier stage, and increase resilience. This is why the Commission, through an **Action Plan to support the protection of public spaces**[3] presented together with this report, set out measures to support Member States at national, regional and local level in their efforts to enhance the physical protection against terrorist threats. While there can never be 'zero risk', the Action Plan seeks to support Member States in detecting threats, reducing the vulnerability of public spaces, mitigating the consequences of a terrorist attack and improving cooperation.

The support the EU can provide to the protection of public spaces is twofold. First, it can foster the **exchange of best practice across borders, including through funding**. This includes, for example, measures to promote and support the development of innovative and discreet barriers to secure cities without changing their open character ("protect by design"). Backing up the measures in the Action Plan with financial support, the Commission today launched a call for proposals through the Internal Security Fund Police for a total amount of EUR 18.5 million. This short-term funding will be complemented in 2018 with funding under Urban Innovative Actions (UIA) as part of the European Regional Development Fund, where security will be a key topic, and for which total funding will be up to EUR 100 million. A public consultation was launched on 15 September 2017 in order to collect ideas from cities on innovative solutions for security. This will help the Commission shape the upcoming calls for proposals in this area.

[3] COM(2017) 612 final (18.10.2017).

Second, the EU can foster **cooperation with a wide range of stakeholders** which is considered crucial to enhance the protection of public spaces. Sharing of experiences and pooling of resources should be better structured. The Commission will set up a forum to engage with private operators, such as shopping malls, concert organisers, sports arenas, hotels and car rental companies. This will facilitate a common awareness of current security challenges and encourage public-private security partnerships to improve protection. Local and regional authorities also have a fundamental role to play in the protection of public spaces, and they need to be associated with related EU-level activities. The Commission will reinforce the involvement of these stakeholders and initiate a dialogue with both regional and local authorities, such as mayors of major cities, to share information and best practice in protecting public spaces. As a follow up to the Nice Declaration[4] of 29 September 2017, early next year the Commission will organise, together with the Committee of the Regions, a high-level meeting with the mayors who signed the Nice Declaration and other interested representatives from local and regional levels to continue the exchange of best practice on the protection of public spaces.

The Commission will also continue its work on the protection and resilience of **critical infrastructure**. The Comprehensive Assessment of EU Security Policy[5] also pointed to a need to adapt the European Programme for Critical Infrastructure Protection[6] to emerging threats. The Commission has started an evaluation of the Directive[7] on the identification and designation of European critical infrastructures. The evaluation will take account of lessons learned and developments over recent years, such as the adoption of the Network Information Security Directive.[8] Meanwhile, the European Programme for Critical Infrastructure Protection has been strengthened, by addressing emerging challenges such as insider threats and hybrid threats, and by widening the external aspect of the programme through cooperation with neighbouring countries in the eastern neighbourhood and the Western Balkans.

---

4 The Declaration of Nice was adopted at a conference of the mayors of the Euro-Mediterranean region in Nice on 29 September 2017, organised at the initiative of the Mayor of Nice, and with the participation of the Commission, to exchange best practice among cities, local and regional levels on the prevention of radicalisation and the protection of public spaces: http://www.nice.fr/uploads/media/default/0001/15/TERRORISME%20EUROPE%20Déclaration%20-%20der%20version.pdf.

5 See the Ninth Progress Report Towards an Effective and Genuine Security Union (COM(2017) 407 final of 26.7.2017) and the annexed Commission Staff Working Document (SWD(2017) 278 final).

6 The European Programme for Critical Infrastructure Protection (EPCIP) sets the framework for EU activities aimed at improving the protection of critical infrastructure in Europe - across all Member States and in all relevant sectors of economic activity. A key pillar of this work is the 2008 Directive on European Critical Infrastructures (Directive 2008/114/EC of 8.12.2008).

7 Directive 2008/114/EC (8.12.2008).

8 Directive 2016/1148 (6.7.2016).

The transport sector has for many years been both the target of terrorist acts, and a means to conduct attacks (e.g. hijacked planes or truck-ramming). In response, there is a need to assess the degree to which **transport security** rules ensure security while also ensuring fluid transport networks. While the aviation sector is significantly better protected, terrorist attacks have become more opportunistic with a greater focus on public spaces. Among these, **rail transport** is a high risk target because its infrastructure is by nature open. There is currently no EU legislative framework to protect passenger rail transport against terrorism and serious crime. On 15 June 2017, the Commission, along with Member States, launched a common railway risk assessment and is working on further measures to improve passenger railway security. The Commission is also working on a best practice security guidance toolkit for the commercial **road transport** sector. This will focus on improving truck security by mitigating the risk of unauthorised intrusion, including hijacking or theft, of a truck for use in a terrorist ramming attack. The toolkit will be available before the end of 2017 and will provide guidance for national road transport sectors. The Commission will also continue work on enhancing **maritime transport security,** in particular to step up the protection of maritime transport infrastructure including ports and ports facilities, container ships and passenger transport ships such as cruises and ferries.

2. Enhanced preparedness against Chemical, Biological, Radiological and Nuclear security risks

Although the likelihood of attacks involving chemical, biological, radiological and nuclear (CBRN) substances in the EU remains low, the overall CBRN threat is evolving. There are indications that certain criminal individuals or terrorist groups may have the intention of acquiring CBRN materials as well as the knowledge and capacity to use them for terrorist purposes. The potential of CBRN attacks features prominently in terrorist propaganda. Also the Comprehensive Assessment of EU Security Policy[9] pointed to a need to step up the preparedness against these threats.

In order to be better prepared to deal with CBRN threats over the coming years, the Commission presents, together with this report, an **Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks**[10]. It includes a wide range of measures to improve preparedness, resilience and coordination at EU level, for example by creating an EU CBRN security network to pool all CBRN actors together. The network will be supported, among others, by a CBRN knowledge hub set up in the European Counter Terrorism Centre (ECTC) in Europol. It is also important to use existing resources better, so the Action Plan proposes strengthening CBRN preparedness and response through training and exercises involving all different first responders (law enforcement, civil protection, health) and – where relevant – military and private partners. It will also be supported by existing tools at EU level, in particular the Union Civil Protection Mechanism (UCPM)[11] and the European Union Agency for Law Enforcement Training (CEPOL). In order to provide better support in the event of a major CBRN incident, Member States should continue strengthening the existing European Emergency Response Capacity (EERC) of the UCPM. In this context, Member States are encouraged to continue committing new capacities to the EERC.

---

[9] See the Ninth Progress Report Towards an Effective and Genuine Security Union (COM(2017) 407 final of 26.7.2017) and the annexed Commission Staff Working Document (SWD(2017) 278 final).

[10] COM(2017 610 final (18.10.2017).

[11] Decision 1313/2013 (17.12.2013).

EU law on **serious cross-border threats to health**[12] provides for preparedness, surveillance, and coordination of responses to health emergencies across the EU. In this context, the EU Early Warning and Response System will be better linked with other EU alert systems on biological, chemical, environmental and unknown threats. The Health Programme is also financing EU-wide exercises on emergency preparedness and response, and joint actions to support Member States in strengthening laboratories, vaccination and core capacities under the International Health Regulations.

All the initiatives will be supported by dedicated research activities, funding and cooperation with relevant international partners.

III. TACKLING THE MEANS THAT SUPPORT TERRORISM

1. Terrorist financing: cross-border access to financial information

Information on the financial activities of terrorist suspects can provide crucial leads in counter-terrorism investigations. Due to its reliability and accuracy, financial data (including data on financial transactions) can help identify terrorists, uncover links with accomplices, establish the activities, logistics and movements of suspects, and map out terrorist networks. Having a rapid overview of the financial activities of suspects and their accomplices can provide law enforcement with crucial information to prevent attacks or react in the aftermath of an attack. The growing phenomenon of crude, small-scale attacks presents new challenges; the indicators of intended plots and acts may be less evident when they are planned at short notice. Financial transactions associated with small-scale plots may not appear suspicious, with the result that this information is only brought to the attention of the competent authorities after an attack.

As announced in the 2016 Action Plan on terrorist financing[13], the **Commission is analysing the need for additional measures** to facilitate access to financial information held in other jurisdictions within the EU for counter-terrorism investigations. In the third progress report towards an effective and genuine Security Union of December 2016[14], the Commission set out its initial analysis and stated that it would continue its assessment, taking particular account of possible impacts on fundamental rights and in particular the right to the protection of personal data. Since then, the Commission has been consulting stakeholders and analysed the mechanisms through which competent authorities can currently access relevant information, particularly financial data stored in other Member States; the obstacles to doing so quickly and effectively; and possible measures to address these obstacles.

In addition to the on-going assessment, the Commission continues to promote the **exchange of best practice** concerning investigation techniques and analyses of terrorist methods to raise and move funds, inter alia through financial support on the basis of a call for proposals of EUR 2.5 million launched today.

---

12 Decision 1082/2013/EU (22.10.2013),
13 COM(2016) 50 final (2.2.2016).
14 COM(2016) 831 final (21.12.2016).

In this context, the Commission is also exploring how to **improve the cooperation between Financial Intelligence Units**[15] established to prevent, detect and effectively combat money laundering and terrorist financing. A mapping report of December 2016 carried out by the Financial Intelligence Units and the related Commission Staff Working Document on improving cooperation between Financial Intelligence Units[16] highlight a number of limitations in the domestic powers of Financial Intelligence Units and outlines a way forward to settle those issues through: (i) implementation of the 4th Anti-Money Laundering Directive[17] and its amendments[18] that are currently being negotiated; (ii) other initiatives carried out by the EU Financial Intelligence Unit Platform in order to enhance operational cooperation, especially through guidance, standardisation work and business solutions to be implemented in FIU.Net; and (iii) regulatory measures to address other issues stemming from the divergent status and competences of Financial Intelligence Units, in particular to facilitate coordination and exchange of information both among Financial Intelligence Units, and between Financial Intelligence Units and law enforcement authorities.

Work is also ongoing to facilitate the **access to financial data within a Member State**. The proposed amendments to the **4th Anti-Money Laundering Directive**[19], currently under negotiation with the co-legislators, would lead to the establishment of central bank account registries or data retrieval systems in all Member States, accessible to Financial Intelligence Units and other competent authorities responsible for money laundering and terrorist financing. These registries, once established in all Member States, will facilitate the detection of account data. Building on that, the Commission is preparing an initiative to **broaden law enforcement access to such bank account registries**[20] to reinforce the capacity of law enforcement authorities to detect the existence of a bank account more rapidly.

---

15 Financial Intelligence Units have been set up by Council Decision 2000/642/JHA (17.10.2000) and are further regulated by Directive 2015/849 (20.5.2015) on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing. They are operationally independent and autonomous units responsible for receiving and analysing suspicious transaction reports and other information relevant to money laundering, associated predicate offences or terrorist financing from relevant entities and for disseminating the results of its analyses and any additional relevant information to the competent authorities.

16 SWD(2017)275 final (26.6.2017).

17 Directive 2015/849 (20.5.2015).

18 COM(2016) 450 final (5.7.2016).

19 COM(2016) 450 final (5.7.2016).

20 http://ec.europa.eu/info/law/better-regulation/initiatives/Ares-2017-3971182.

During consultations with stakeholders **obstacles to obtaining financial transaction data held in other Member States** have also been raised. Where necessary, bank account information can be exchanged between Member States through police cooperation channels within eight hours.[21] Access to financial transaction data held by other Member States can also be facilitated through Financial Intelligence Units. When such information needs to be used as evidence in criminal proceedings, it might need to be requested through mutual legal assistance. The European Investigation Order[22] offers new possibilities to obtain financial transaction data in a manner substantially quicker than through mutual legal assistance. To date, a few months after the transposition deadline, only 16 Member States have transposed the European Investigation Order and the remaining Member States are urged to do so without further delay. Finally, the upcoming legislative proposals on electronic evidence foreseen for early 2018 will also facilitate cross-border access to such data.

Consultations with stakeholders point also **to obstacles that hamper the detection of financial transaction data held in other Member States**. As a step to address this and as part of its on-going assessment, the Commission will assess the necessity, technical feasibility and proportionality of interconnecting centralised bank account registers, taking into account all existing and planned instruments to facilitate access to financial transaction data held in other Member States.

To that end, the Commission will **continue to consult with all stakeholders** concerned on the necessity, technical feasibility and proportionality of possible new measures at Union level to facilitate and speed up cross-border access to financial transaction data, including procedures to ensure confidentiality. Bringing together the on-going assessments related to the use of financial information for counter-terrorism investigations, the Commission will organise a high-level stakeholder meeting in November 2017. The central points for discussion will include:

- the main obstacles for effective and timely access to financial transaction data held in other Member States for counter-terrorism investigations;
- the necessity, technical feasibility and proportionality of possible additional measures to facilitate cross-border access to financial transaction data for counter-terrorism investigations in a quick, effective and secure manner.

The Commission will report on the outcome of this discussion.

---

21 Council Framework Decision 2006/960/JHA (the "Swedish Initiative") foresees the following time limits for law enforcement authorities to respond to foreign requests: eight hours in urgent cases when the requested information or intelligence is held in a database directly accessible by a law enforcement authority; and longer time limits when the requested information or intelligence is not held in a database directly accessible.

22 Directive 2014/41 (3.4.2014).

2. Explosives: further restricting access to explosives precursors

The **Regulation on Explosives Precursors**[23] restricts the general public's access to, and use of, seven chemical substances (the so-called 'restricted explosives precursors' listed in Annex I of the Regulation). In February 2017, the Commission adopted a report on the application of the Regulation by Member States.[24] This report concluded that the implementation of the Regulation has contributed to reducing access to dangerous explosive precursors that can be misused to manufacture homemade explosives. Member States have also reported examples where the application of the Regulation has led to the early identification of terrorist plots.[25] To ensure the full implementation of the Regulation, the Commission launched infringement procedures in May and September 2016 against a number of Member States for failing to implement fully the Regulation. As of October 2017, only two infringements are still open against Spain and Romania.

Despite these joint efforts, recent terrorist attacks and incidents indicate that the **threat posed by home-made explosives** in Europe remains high. These substances continue to be accessed and used for the purpose of making home-made explosives. The explosive used in most of the attacks was triacetone triperoxide (TATP), a home-made explosive that is reported to be the explosive of choice for terrorists.[26]

Given the present threat from explosive precursors, it is necessary to take immediate measures to ensure the current Regulation is implemented by all Member States to best effect. This is why the Commission issued, together with this report, a **Recommendation**[27] giving its guidance on immediate steps to prevent misuse of explosives precursors. The Commission encourages Member States to implement fully this Recommendation in order to restrict as much as possible the access to and use of explosives precursors by terrorists and ensure that controls on legitimate use, and action in case of suspicious transactions, are improved. The Commission stands ready to assist Member States in doing so.

In addition, the Commission is stepping-up its **review of the Regulation on Explosives Precursors** with an evaluation that will be followed by an impact assessment during the first half of 2018. The evaluation will examine the relevance, effectiveness, efficiency, coherence and added value of the Regulation, and identify problems and obstacles that might require further action. The impact assessment will examine various policy options to address any problems and obstacles identified.

---

23 Regulation 98/2013 (15.1.2013).

24 COM(2017) 103 final (28.2.2017).

25 On 23 June 2017, the Belgian ministry of interior announced that, in one year, they had received 30 reports concerning suspicious sales. From February to June 2017, France has received 11 reports involving, for the most part, hydrogen peroxide.

26 EU Terrorism Situation and Trend Report (TE-SAT) 2017: https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017.

27 C(2017) 6950 final (18.10.2017).

3. Encryption: supporting law enforcement in criminal investigations

The use of encryption is essential to ensure cybersecurity and the protection of personal data. EU legislation specifically notes the role of encryption in ensuring appropriate security for the processing of personal data.[28] At the same time, in the context of criminal investigations, law enforcement and judicial authorities increasingly encounter challenges posed by the use of encryption by criminals. This affects the ability of law enforcement and judicial authorities to obtain the information needed as evidence in criminal investigations, and to prosecute and convict criminals. The use of encryption by criminals, and therefore its impact on criminal investigations, is expected to continue to grow in the coming years.

Following a call from the Justice and Home Affairs Council in December 2016, the Commission has **discussed the role of encryption in criminal investigations with relevant stakeholders**, addressing both technical and legal aspects. This included experts from Europol, Eurojust, the European Judicial Cybercrime Network (EJCN), the European Union Agency for Network and Information Security (ENISA), the European Union Agency for Fundamental Rights (FRA) and Member States' law enforcement agencies, industry and civil society organisations. Progress was regularly reported at Council working group level, and a workshop with Member States took place on 18 September 2017. Several roundtables with industry and civil society organisations were held throughout the process.

Following these discussions with Member States and stakeholders and based on their input, the Commission concludes that the following set of **measures to support law enforcement and judicial authorities** when they encounter the use of encryption by criminals in criminal investigations should be implemented. This includes (a) legal measures to facilitate access to encrypted evidence as well as (b) technical measures to enhance decryption capabilities. The Commission will continue to monitor the developments in this regard.

(a) legal framework for cross-border access to electronic evidence

Law enforcement authorities often face the challenge of access to evidence located in another country. Ongoing legislative developments at European level can support law enforcement and judicial authorities in their ability to obtain access to necessary, but possibly encrypted, information located in another Member State. Effective investigation and prosecution of crimes need an appropriate framework. To this end, the Commission will in early 2018 bring forward proposals to facilitate **cross-border access to electronic evidence**. In parallel, the Commission is implementing a set of practical measures[29] to improve cross-border access to electronic evidence for criminal investigations, including funding for training on cross-border cooperation, the development of an electronic platform to exchange information within the EU, and the standardisation of judicial cooperation forms used between Member States.

[28] Article 32 of Regulation 2016/679 (27.4.2017).

[29] See the Eighth Progress Report towards an Effective and Genuine Security Union (COM(2017) 354 final of 29.6.2017).

(b) technical measures

Depending on how encryption is used by criminals, law enforcement and judicial authorities may be able to recover some of the information. A number of Member States have established national services with expertise on the challenge of encryption in the context of criminal investigations. However, most Member States do not have access to the right level of expertise and technical resources. This seriously challenges law enforcement and judicial authorities' ability to access encrypted information in criminal investigations. This is why the Commission is proposing a **range of measures to support Member State authorities**, without prohibiting, limiting or weakening encryption.

First, the Commission will support **Europol** to further develop its decryption capability. To that end, the Commission proposed, in the context of the preparation of the EU Budget for 2018, a total of 86 additional security-related posts for Europol (19 more than in the 2017 budget), in particular to reinforce Europol's European Cybercrime Centre (EC3). The need for additional resources will be assessed, and the Commission will report in the next Security Union Progress Report on the funds made available to this end. Future technological developments should be taken into account on the basis of research and development under the Horizon 2020 programme and other EU-funded programmes. Measures that could weaken encryption or could have an impact on a larger or indiscriminate number of people would not be considered.

Second, to support law enforcement and judicial authorities at national level, a **network of points of expertise** should be established. Without replacing national initiatives, capabilities and expertise at national level could be better shared. Member States are encouraged to use funding under national programmes of the Internal Security Fund Police (ISF-P) programme to create, extend or develop national expertise points. At European level, the Commission will support Europol in providing the functions of a network hub to facilitate collaboration among these national expertise points.

Third, Member State authorities should have a **toolbox of alternative investigation techniques** at their disposal to facilitate the development and use of measures to obtain needed information encrypted by criminals. The network of points of expertise should contribute to developing the toolbox and the European Cybercrime Centre (EC3) at Europol is best-placed to set up and keep a repository of those techniques and tools. Measures that could weaken encryption or could have an impact on a larger or indiscriminate number of people would not be considered.

Fourth, attention should be paid to the **important role of service providers and other industry partners** in providing solutions with strong encryption. Considering the Commission's commitment to strong encryption, a better and more structured collaboration between authorities, service providers and other industry partners would promote a better understanding of the existing and evolving challenges on the various sides. The Commission will support structured dialogues with service providers and other businesses under the umbrella of the EU Internet Forum and the network of points of expertise, and where appropriate with the involvement of civil society.

Fifth, **training programmes** for law enforcement and judicial authorities should ensure that responsible officers are better prepared to obtain necessary information encrypted by criminals. To support the development of training programmes, the Commission intends to provide funding of EUR 500,000 under the 2018 annual work programme of the Internal Security Fund Police. The expertise of the European Cybercrime Training and Education Group (ECTEG) will be taken into account where relevant. The Commission will also support the delivery of training by the European Union Agency for Law Enforcement Training (CEPOL) and Member States are encouraged to use for training the funding available under their national programmes of the Internal Security Fund Police.

Sixth, there is a need for **continuous assessment of technical and legal aspects** of the role of encryption in criminal investigations given the constant development of encryption techniques, their increased use by criminals and the effect on criminal investigations. The Commission will continue this important work. It will also support the development of an observatory function in collaboration with the European Cybercrime Centre (EC3) at Europol, the European Judicial Cybercrime Centre (EJCN) and Eurojust.

IV. Countering radicalisation

1. High Level Expert Group on Radicalisation

Recent attacks, especially by lone actors, and the speed in the way some of the perpetrators were radicalised have served as sharp reminders of the importance of preventing and countering radicalisation. The Commission set up a **High Level Expert Group on Radicalisation** to step up efforts to prevent and counter radicalisation and to improve coordination and cooperation between all relevant stakeholders building on achievements so far.[30] The Group is tasked with setting out recommendations for further work in this area, with a first interim report to be completed this year. The Commission will report to the Justice and Home Affairs Council in December 2017 on the progress made. The Group will also address the framework conditions necessary to strengthen capacity and know-how on anti-radicalisation, including the possible need for further cooperation structures at EU level. In that respect, some Member States have called for an EU Centre for the Prevention of Radicalisation, and the Group will look into the need and added value of establishing such a structure.

Among the priority issues to be discussed by the Group is **radicalisation in prisons**. The current focus is on implementation by the Member States of the JHA Council Conclusions on enhancing the criminal justice response to radicalisation of 20 November 2015.[31] The Commission will organise a stakeholder conference on the criminal justice response to radicalisation on 27 February 2018 to share the results of ongoing projects.

The Commission will take the conclusions and recommendations of the Group into account in the work plan of existing initiatives (in particular within the Radicalisation Awareness Network Centre of Excellence), as well as in the use and focus of its funding instruments (including the Internal Security Fund, but also other related funds such as Erasmus+, the Justice programme or the European Social Fund).

---

[30] See the Eighth Progress Report towards an Effective and Genuine Security Union (COM(2017) 354 final of 29.7.2017).

[31] Conclusions of the Council of the European Union and of the Member States meeting within the Council on enhancing the criminal justice response to radicalisation leading to terrorism and violent extremism (14382/15).

2. Countering online radicalisation

Terrorists continue to use the Internet to radicalise, recruit, prepare and incite attacks as well as to glorify their atrocities. The European Council[32], the G7[33] and the G20[34] recently urged further action to address this global challenge and recalled the industry's responsibility in that respect.

In July 2017, the EU Internet Forum set out an **Action Plan to combat terrorist content online**, calling on the internet industry to take decisive action, devote resources and develop the necessary technological tools to ensure the swift detection and take-down of harmful material. The Action Plan calls for immediate progress on a wide range of areas[35] and sets up a regular reporting mechanism to measures and assess results.

On 29 September 2017, the Commission hosted a senior officials' meeting of the EU Internet Forum to take stock of the **implementation of the Action Plan to combat terrorist content online**. With regards to automated detection, more companies are moving in this direction allowing them to deploy technical expertise to identify terrorist content at the point at which it is uploaded. Some companies reported that 75% of content is now detected automatically, and referred to human reviewers for the final decision on removal, whereas for others 95% of content is now detected via proprietary detection tools. While this represents concrete progress, the Commission has urged all companies to step up the deployment of these tools to ensure faster detection, reduce the amount of time terrorist content remains online, and faster and more effective removal of terrorist propaganda. The Commission has also urged companies to expand their 'database of hashes' tool to ensures that removed terrorist content is not re-uploaded on other platforms, thereby stemming the dissemination of terrorist content across multiple platforms. This tool should be extended in terms of content it includes – beyond video and images that are currently covered – and in terms of the participating companies.

The Commission also continues to support civil society organisations to spread positive **counter-narrative messages** online. The Commission launched on 6 October 2017 a call for proposals to provide funding of EUR 6 million to consortia of civil society actors that develop and implement such campaigns.

Looking ahead, on 6 December 2017, the European Commission will convene the **EU Internet Forum at Ministerial level** with the participation of high-level representatives of the internet industry to assess progress and pave the way for future action.

32 http://www.consilium.europa.eu/en/meetings/european-council/2017/06/22-23-euco-conclusions_pdf/.
33 http://www.consilium.europa.eu/en/press/press-releases/2017/05/26-statement-fight-against-terrorism/.
34 http://www.consilium.europa.eu/en/press/press-releases/2017/07/07-g20-counter-terrorism/.
35 COM(2017) 407 final (26.7.2017).

The actions taken against terrorist content online in the framework of the EU Internet Forum should be seen in the wider framework of tackling illegal content on the internet. These actions were reinforced by a Communication adopted by the Commission on 28 September 2017 setting out **guidelines and principles for online platforms** to step up the fight against illegal content online[36] in cooperation with national authorities, Member States and other relevant stakeholders. The Communication aims to facilitate and intensify the implementation of good practices for preventing, detecting removing and disabling access to illegal content to ensure the effective removal of illegal content, increase transparency and protect fundamental rights. It also aims to provide clarifications to platforms on their liability when they take proactive steps to detect, remove or disable access to illegal content. The Commission expects online platforms to take swift action over the coming months, including in the context of relevant dialogues such as the EU Internet Forum for terrorism and illegal hate speech.

In parallel, the Commission will monitor progress and assess whether additional measures are needed, in order to ensure the swift and proactive detection and removal of illegal content online, including possible legislative measures to complement the existing regulatory framework. This work will be completed by May 2018.

In legislative terms, the Commission proposal[37] for the **revision of the Audiovisual Media Services Directive (AVMSD)**, tabled in May 2016, reinforces the fight against hate speech. It seeks to align the Directive with the Framework Decision on combating certain forms and expressions of racism and xenophobia[38] and the Charter of Fundamental Rights. It also foresees an obligation on Member States to ensure that video-sharing platforms put in place appropriate measures to protect all citizens from incitement to violence or hatred. These measures consist, for instance, of flagging and reporting mechanisms.

V. EXTERNAL DIMENSION OF COUNTER-TERRORISM

1. EU external action on counter-terrorism

The EU's external action on countering terrorism contributes to the priority objective of strengthening the Union's internal security. Therefore, the strategic and policy continuum between EU's internal and external security should be further reinforced to enhance the effectiveness of counter-terrorism actions across the board.

The Commission supports a large spectrum of external actions to enhance security, with funding of more than EUR 2.3 billion made available for more than 600 projects on-going as of 1 January 2017. A number of activities are either security-focused (i.e. specific actions in matters such as fighting terrorist financing, countering radicalisation, borders, prisons) or security-relevant (i.e. programmes that address root causes of insecurity and grievances by helping to improve education, access to natural resources and energy, governance and the security sector, support to civil society).

---

36 Communication on Tackling Illegal Content Online, 'Towards an enhanced responsibility of online platforms' (COM(2017) 555 final of 28.9.2017).

37 COM(2016) 287 final (25.5.2016).

38 Council Framework Decision 2008/913/JHA (28.11.2008).

The Foreign Affairs Council of 19 June 2017 renewed the strategic direction in these fields by adopting comprehensive **Conclusions on EU External Action on Counter-Terrorism**[39]. The High Representative and the European Commission will jointly work as necessary towards the successful implementation of these Conclusions. To ensure timely and comprehensive implementation of the Conclusions and reporting to the Council by June 2018, a joint coordination process between the European External Action Service and the European Commission has been put in place. Priority will be given to:

- **Strengthening the network of counter-terrorism experts in EU Delegations**: Counter-terrorism experts should increasingly be involved in the programming of EU support and in the local coordination of Member States' individual counter-terrorism cooperation with our partners. To promote this enhanced role, training before and during deployment of these experts will be stepped up. Their tasking will be made more focused with specific mission letters and their liaison to the EU Justice and Home Affairs Agencies will be made more stable. In order to cover all high-priority areas, the network of counter-terrorism experts[40] will be expanded to the Horn of Africa, Central Asia and South-East Asia.
- **Enhancing cooperation between Common Security and Defence Policy missions and operations and EU Justice and Home Affairs Agencies** in respect of the collection, analysis and exchange of information, and further exploring how to enhance linkages between military and law enforcement actors for counter-terrorism purposes. To enhance data and information exchange between Common Security and Defence and justice and home affairs policies, it will be important to foster a revision of elements of the current regulatory frameworks and pilot the embedding of Crime Information Cells in selected Common Security and Defence Policy missions and operations. It will be important to further facilitate and improve linkages with EU Justice and Home Affairs Agencies' activities in priority third countries, including where possible enhancing information-sharing between EU and non-EU actors.
- **Strengthening international cooperation in counterterrorism and the prevention and countering of violent extremism** with partner countries in the Western Balkans, the Middle East, North Africa, Turkey, the Gulf, the Sahel and the Horn of Africa; with key strategic partners, including the United States, Canada and Australia; and with key regional and multilateral partners as the United Nations, NATO, the Global Counterterrorism Forum, the Financial Action Task Force, the African Union, the Association of South-East Asian Nations, the Gulf Cooperation Council and the League of Arab States.

---

39 http://www.consilium.europa.eu/en/press/press-releases/2017/06/pdf/Read-the-full-text-of-the-Council-conclusions_pdf(4)/.

40 To date, the EU deploys Counter-Terrorism Experts to its Delegations in: Algeria, Bosnia and Herzegovina (with regional mandate for the Western Balkans), Chad (Sahel), Iraq, Jordan, Lebanon, Libya (stationed in Tunis), Morocco, Nigeria, Pakistan, Saudi Arabia, Tunisia and Turkey.

2. Council of Europe Convention on the Prevention of Terrorism

To step up international cooperation on counter-terrorism, the Commission is putting forward, alongside this report, **proposals[41] for Council Decisions on the conclusion of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol**. The Convention[42], adopted by the Council of Europe on 16 May 2005, relates to the criminalisation of terrorist and terrorist-related activities, to international cooperation regarding such offences and to protection, compensation and support for victims of terrorism. The Convention came into force on 1 June 2007. All EU Member States have signed the Convention and 23 EU Member States have ratified it. The objective of the Additional Protocol[43], adopted by the Council of Europe on 18 May 2015, is to supplement the Convention with a series of provisions aimed at implementing the criminal law aspects of UN Security Council Resolution 2178(2014)[44] on "Threats to international peace and security caused by terrorist acts". The Additional Protocol responds to this Resolution by furthering a common understanding of and response to offences related to foreign terrorist fighters. The Additional Protocol came into force on 1 July 2017.

The EU signed the Convention and its Additional Protocol on 22 October 2015. Given that the EU has adopted a comprehensive set of legal instruments to counter terrorism, notably with the Directive on Combating Terrorism,[45] the EU is now ready to complete its commitment to become a party to the Convention and its Additional Protocol.

3. Towards a revised passenger name record agreement with Canada

In its Opinion of 26 July 2017[46] the Court of Justice of the EU stated that the Agreement between Canada and the EU for the transfer and use of passenger name record (PNR) data signed on 25 June 2014 cannot be concluded in its current form because several of its provisions are incompatible with the fundamental rights recognised by the EU, in particular the right to data protection and respect for private life. The Commission is now in contact with Canada, including in the margins of the upcoming G7 Interior Ministers' Meeting in Ischia on 19/20 October 2017, to prepare the upcoming negotiations to revise the text of the Agreement. To this end, the Commission submitted, together with this report, a **Recommendation[47] to the Council to authorise the opening of negotiations for a revised Agreement** in line with all the requirements set by the Court in its Opinion. The Council is invited to swiftly authorise the opening of such negotiations. Given that the use of PNR data is an important tool to fight terrorism and serious transnational crime, the Commission will take the necessary steps to ensure the continuation of PNR data transfers to Canada in full respect of fundamental rights in compliance with the Court's Opinion.

In this context, the Commission underlines its continuing support to Member States in implementing the EU PNR Directive[48]; the obligations on Member States deriving from that Directive are unaffected by the Court's Opinion.

---

41 COM(2017) 606 final (18.10.2017) and COM(2017) 607 final (18.10.2017).
42 https://rm.coe.int/168008371c.
43 https://rm.coe.int/168047c5ea.
44 http://www.un.org/en/sc/ctc/docs/2015/SCR%202178_2014_EN.pdf.
45 Directive 2017/541 (15.3.2017).
46 Opinion 1/15 of the Court of Justice (26.7.2017).
47 COM(2017) 605 final (18.10.2017).
48 Directive 2016/681 (27.4.2016).

4. Strengthening Europol's cooperation with third countries

Cooperation with third countries is essential in the fight against terrorism and organised crime, as underlined by the June 2017 Foreign Affairs Council Conclusions on EU External Action on Counter-Terrorism[49] and relevant EU regional strategies.[50] Before the new Europol Regulation[51] entered into force on 1 May 2017, Europol had concluded under its previous legal basis[52] agreements with a number of third countries to ensure a cooperation framework for the exchange of strategic and technical information. Some of these agreements also include the possibility to exchange personal data.[53] These agreements remain in force.

Since 1 May 2017 the new **Europol Regulation** determines the rules for Europol's external relations with third countries, in particular the conditions for the exchange of personal data with Union bodies, third countries and international organisations. Pursuant to the Treaty and the Regulation, the Commission is responsible, on behalf of the Union, for negotiating international agreements with third countries for the exchange of personal data with Europol.[54] In so far as necessary for the performance of its tasks, Europol may establish and maintain cooperative relations with external partners through working and administrative arrangements that do not allow the exchange of personal data.

In the light of the Union's operational needs in terms of security cooperation with third countries, and in line with the Europol Regulation, the **Commission will put forward recommendations to the Council before the end of the year** to authorise the opening of negotiations for agreements between the EU and Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey to provide a legal basis for the transfer of personal data between Europol and these third countries.[55] Such agreements will further strengthen Europol's capabilities to engage with these third countries for the purposes of preventing and combatting crimes falling within the scope of Europol's objectives.

---

49 http://www.consilium.europa.eu/en/press/press-releases/2017/06/pdf/Read-the-full-text-of-the-Council-conclusions_pdf(4)/.

50 This includes the revised European Neighbourhood Policy (JOIN(2015) 50 final of 18.11.2015).

51 Regulation 2016/794 (11.5.2016).

52 Council Decision 2009/371/JHA (6.4.2009).

53 Europol concluded agreements allowing for the exchange of personal data with the following third countries: Albania, Australia, Bosnia and Herzegovina, Canada, Colombia, Former Yugoslav Republic of Macedonia, Georgia, Iceland, Liechtenstein, Moldova, Monaco, Montenegro, Norway, Serbia, Switzerland, Ukraine and the United States. Europol's Management Board had authorised the opening of negotiations on an agreement between Europol and Israel but these negotiations were not concluded when the new Europol Regulation entered into application.

54 The Europol Regulation also provides for the transfer of personal data between Europol and a third country on the basis of a Commission decision finding that the country in question ensures an adequate level of data protection ('adequacy decision').

55 Beyond these third countries, the Commission recalls the strategic framework for 'adequacy decisions' as well as other tools for data transfers and international data protection instruments, as articulated in the Commission Communication on Exchanging and Protecting Personal Data in a Globalised World (COM(2017) 7 final of 10.1.2017) in which the Commission encourages accession by third countries to Council of Europe Convention 108 and its additional Protocol.

VI. CONCLUSION

This report sets out a package of anti-terrorism measures that will further support Member States in their efforts to address current security threats. The Commission encourages Member States and the Council to implement these measures as a matter of priority. The Commission will keep the European Parliament and the Council informed of progress made.

The next Security Union progress report will be presented in December 2017, with a focus on the interoperability of EU information systems for security, border and migration management. In this context the Commission recalls the importance of making progress on legislative priorities on these information systems.