



Strasbourg, 17.4.2018
COM(2018) 211 final

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

Fourteenth progress report towards an effective and genuine Security Union

I. INTRODUCTION

This is the fourteenth Progress 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.

The brutal attacks in Trèbes and Carcassonne, France, on 23 March 2018 are a reminder that the threat from terrorism remains high in the EU. As part of continued efforts in the Security Union to counter this threat, the Commission presented, together with this Progress Report, a new security package with measures to close down the space in which terrorists and other criminals operate, making it more difficult for them to plan and execute their heinous acts. It includes legislative proposals to improve cross-border gathering of **electronic evidence** and access to **financial information** for investigations and prosecution, in particular for serious crimes, also strengthening cooperation between Financial Intelligence Units and law enforcement authorities. The package also includes operational measures to prevent the access of terrorists and other criminals to imported **firearms** and **explosives precursors** that can be misused to make homemade explosives, as experienced in several recent attacks. Finally, a legislative proposal to improve the **security of national identity cards and residence documents** will make it more difficult for terrorists and other criminals to misuse or falsify such documents to enter or move within the EU.

The 4 March 2018 attack in Salisbury has given a shocking example of the genuine threat chemical substances can pose to collective security. The 22-23 March 2018 European Council condemned the attack in the strongest possible terms. It underlined that, as part of the response, the EU must step up its resilience to chemical, biological, radiological and nuclear-related risks. This Progress Report sets out the measures that are being taken to that end, implementing the October 2017 Action Plan to enhance preparedness against these security risks. This Progress Report also provides an update on the implementation of other priority files in the Security Union, covering efforts to counter radicalisation online, to enhance information sharing, to support the protection of public spaces and to counter cyber threats.

II. CLOSING DOWN THE SPACE IN WHICH TERRORISTS AND CRIMINALS OPERATE

1. New tools to gather electronic evidence in criminal proceedings

Electronic evidence has become relevant in a large majority of criminal investigations and increasingly often, judicial authorities need to make a request in another jurisdiction in order to obtain necessary evidence from service providers. Making it easier and quicker to obtain this evidence across borders is therefore of crucial importance for investigating and prosecuting crime, including terrorism or cybercrime. To this end, the Commission presented, together with this Progress Report, two legislative proposals to improve the cross-border gathering of electronic evidence for criminal proceedings, namely a proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters¹ and a proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings². The proposed Regulation and Directive will provide competent law enforcement and judicial authorities

¹ COM(2018) 225 final (17.4.2018).

² COM(2018) 226 final (17.4.2018).

with new tools to obtain electronic evidence for the investigation and prosecution of crimes, including terrorism and cybercrime. With these proposals, the Commission is responding to calls from the European Parliament and the Council to put forward a legislative framework at EU level for measures to obtain electronic evidence across borders, along with robust safeguards to protect the rights and freedoms of individuals.³

The proposed Regulation provides for a European Production Order and a European Preservation Order. These Orders will allow competent authorities from one Member State to directly compel service providers (providers of electronic communications services and specific providers of information society services) established or represented in another Member State to preserve or produce existing electronic data for the investigation and prosecution of crimes falling within the scope of the Regulation, in a way that is proportionate and necessary in the individual case. In order to ensure compliance with these orders, the proposed Directive obliges service providers to designate at least one legal representative in the Union. In view of the borderless nature of the internet, the proposals cover relevant service providers that offer services in one or more Member States, irrespective of the location of their headquarters, their infrastructure or the storage of the information.

The proposed Regulation provides strong safeguards to ensure full compliance with fundamental rights, such as the ex-ante involvement of judicial authorities and additional requirements for obtaining certain data categories. Moreover, since the Orders can only be issued in the framework of criminal proceedings and if provided for in comparable national situations, all criminal law procedural safeguards apply. In addition, the Regulation provides specific rules for effective remedies for individuals affected. The Regulation also includes a right for the service provider to request review in the issuing Member State or, if the Order is transmitted for enforcement, in the host Member State, on the basis of defined grounds. This includes cases where it is apparent that the Order was not issued or validated by a competent authority, is incomplete, manifestly violates the Charter of Fundamental Rights of the European Union or is manifestly abusive. In addition, the Regulation provides for mechanisms to avoid and mitigate potential conflicts with obligations that service providers may have under third countries' laws.

The legislative proposals are based on a thorough impact assessment and have been informed by a two-year consultation process that has involved practitioners, citizens, service providers, governmental and non-governmental organisations and academics.⁴ The Commission has also participated in related discussions in the Council of Europe and has closely followed developments in non-EU countries, including the recent adoption by the United States Congress of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). The proposals adopted together with this Progress Report provide a basis for a coordinated and coherent approach both within the EU and by the EU at international level, with due regard to EU rules, including on non-discrimination between EU Member States and their nationals. The Commission also continues to participate actively in the discussions within the framework of the Council of Europe Convention on cybercrime.

³ Council Conclusions on improving criminal justice in cyberspace (ST 9579/16) and European Parliament Resolution of 3 October 2017 on the fight against cybercrime (2017/2068 (INI)).

⁴ The consultation report is available at https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en; more resources can be found on https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.

The Commission calls on the co-legislators to examine this proposed legislation, which is included in the Joint Declaration on the EU's legislative priorities for 2018-2019, without delay with a view to reaching swift agreement.

In parallel to the legislative proposals, the Commission continues to work on **practical measures to improve judicial cooperation** based on Mutual Legal Assistance and the Directive on a European Investigation Order⁵ as well as the cooperation between authorities and service providers within the existing legal framework. These measures include training for authorities, fostering the use of single points of contact at national level and creating an online platform for the secure exchange of European Investigation Order requests and responses based on an electronic version of the European Investigation Order forms. The Commission is working closely with relevant EU Agencies⁶ and stakeholders to ensure their swift implementation.

2. *Facilitating the use of financial information for the prevention, detection, investigation or prosecution of serious criminal offences*

Criminals and terrorists operate across different Member States and are able to transfer funds between different bank accounts in a matter of hours to prepare their acts or to move and launder proceeds of crime. Investigations into serious crimes and terrorism may come to a dead end because of failure to secure timely, accurate and comprehensive access to the relevant financial data.⁷ Given the importance of financial information for investigations, it is crucial to step up the cooperation between the authorities responsible for combating serious crime and terrorism and enhance their access to and use of financial information, in full respect of fundamental rights and the applicable procedural safeguards. To that end, the Commission adopted together with this Progress Report a **proposal for a Directive to facilitate the use of financial and other information** for the prevention, detection, investigation or prosecution of serious criminal offences.⁸

The proposal, based on a thorough impact assessment, gives designated law enforcement authorities and Asset Recovery Offices direct **access to bank account information** held in national centralised bank account registries and data retrieval systems as established under the Anti-Money Laundering Directive.⁹ Such access will be granted on a **case-by-case basis for the purposes of combating serious crime**. This will also considerably decrease the administrative burden on financial institutions which will no longer have to respond to blanket requests for information from law enforcement authorities.

The proposal further strengthens cooperation between national **Financial Intelligence Units** and law enforcement authorities, as well as between Financial Intelligence Units in different

⁵ Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, p. 1–36.

⁶ Europol, Eurojust and the European Union Agency for Law Enforcement Training (CEPOL).

⁷ The Europol Report “From suspicion to action: converting financial intelligence into greater operational impact”, which was published in 2017, highlighted these problems and the need for better access of law enforcement authorities to financial information.

⁸ COM(2018) 213 final (17.4.2018).

⁹ The Union co-legislators agreed in December 2017 on this as one of the changes to the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141 of 5.6.2015, p. 73).

Member States. In addition, Member States will need to ensure that their Europol National Unit replies to requests by Europol for information contained in centralised bank account registries and for financial information and financial analyses. Requests made by Europol will have to be duly justified and provided on a case-by-case basis, within the limits of Europol's responsibilities and for the performance of its tasks. Better access by law enforcement authorities to financial data and better cooperation with Financial Intelligence Units will speed up investigations and enable the authorities to combat cross-border crime more effectively. Europol will also be able to enhance its support to Member States in fighting criminal offences falling within Europol's competence. In order to comply with the fundamental rights to the protection of personal data and to privacy, the proposal for a Directive provides for strict safeguards for the processing of personal data.

The Commission calls on the co-legislators to examine the proposal, which is included in the Joint Declaration on the EU's legislative priorities for 2018-2019, without delay in order to reach swift agreement. The Commission also reiterates the importance of fully implementing and applying the Fourth Anti-money Laundering Directive and the tools it provides to counter money laundering and terrorist financing. This includes the need to provide Financial Intelligence Units with adequate resources to fulfil their tasks. Moreover, the amendment to the Fourth Anti-money Laundering Directive – politically agreed by the co-legislators in December 2017 – requires the Commission to submit, by June 2020, a report to the European Parliament and to the Council assessing the possible future interconnection of centralised bank account registries. The Commission is carrying out a study to that end and will present its findings by mid-2019.

3. Strengthened rules against explosives precursors used for homemade explosives

Terrorists and criminals have used homemade explosives in many attacks in the EU, including those in Madrid (2004), London (2005), Paris (2015), Brussels (2016), Manchester (2017) and Parsons Green (2017). An even higher number of failed and foiled attacks also involved the attempted use of homemade explosives. These attacks underline the need to restrict as much as possible terrorists' access to and use of explosives precursors that can be misused to make homemade explosives. To that end, the Commission adopted, together with this Progress Report, a **proposal¹⁰ to revise and strengthen the existing restrictions of Regulation 98/2013 on the marketing and use of explosives precursors.**¹¹ This follows up on the Commission Recommendation¹² of October 2017 that set out immediate actions to prevent misuse of explosives precursors on the basis of existing rules. The proposal is based on a number of consultations of different stakeholder groups and a thorough impact assessment. Under the 2013 Regulation, the making available, introduction, possession and use of certain explosives precursors is restricted and suspicious transactions need to be reported. Although these restrictions and controls have helped to decrease the amount of explosives precursors available to the general public and led to an increase in the number of reports on suspicious transactions, they have proven to be insufficient to prevent the misuse of these substances by terrorists and criminals to produce explosives.

The Commission's proposal will help to close these security gaps and to strengthen and clarify the legal framework. The proposed Regulation (that will replace the previous Regulation of

¹⁰ COM(2018) 209 final (17.4.2018).

¹¹ Regulation (EU) No 98/2013 of the European Parliament and of the Council of 15 January 2013 on the marketing and use of explosives precursors, OJ L 39, 9.2.2013, p. 1–11.

¹² Commission Recommendation of 18.10.2017 on immediate steps to prevent misuse of explosives precursors (C (2017) 6950 final).

2013) will aim to further restrict access to dangerous explosives precursors for the general public through a number of measures. It will add two additional substances¹³ to the list of restricted explosive precursors, limit the possibility to apply for a licence to fewer substances, and reinforce mandatory checks of the applicant's criminal records. The registration system of the 2013 Regulation will be discontinued given that it provides less security. Moreover, the proposal clarifies that rules applicable to economic operators will also fully apply to online sales. The proposed Regulation will improve enforcement by the competent authorities and the transmission of information along the supply chain. In doing so, the proposed Regulation will make it significantly more difficult for terrorists to produce home-made explosives. The Commission invites the co-legislators to examine the legislative proposal without delay in order to reach swift agreement.

4. *Improved security of identity cards and residence documents to prevent document fraud and the use of false identities*

As demonstrated by the European Border and Coast Guard Agency's statistics on fraudulent documents, national identity cards with weak security features are the most often fraudulently used travel documents within the EU. As part of the European response to travel document fraud set out in the December 2016 Action Plan¹⁴, the Commission adopted together with this Progress Report a **proposal for a Regulation to strengthen the security of identity cards issued to Union citizens and of residence documents issued to Union citizens and their family members**.¹⁵ In accordance with EU free movement law, EU citizens can use national identity cards as travel documents, both when travelling within the EU and when crossing the EU external borders to return to the EU. In certain cases, EU citizens can use national identity cards in order to enter third countries. Residence cards of non-EU family members used together with a passport grant the right to enter the EU without a visa when accompanying an EU citizen. EU law already provides for standards for security features and biometrics (facial image and fingerprints) in passports and travel documents issued by Member States.¹⁶

Enhancing the security features of identity cards and residence documents will make it more difficult for criminals to misuse or falsify such documents to move within the EU or cross the EU external borders. More secure identity documents will contribute to strengthening EU external border management (including as regards the challenge of returning foreign terrorist fighters and their family members), while at the same time, more secure and reliable documents will make it easier for EU citizens to exercise their free movement rights.

The Commission proposal, based on a thorough impact assessment and public consultation, therefore sets out minimum document security standards for national identity cards, including in particular a biometric photo and fingerprints to be stored in a chip on the identity card. The proposal also foresees minimum information to be provided on the residence documents issued to mobile EU citizens, as well as full harmonisation of the residence cards of non-EU family members.

The Commission calls on the co-legislators to examine the legislative proposal without delay in order to reach swift agreement.

¹³ Sulphuric acid and ammonium nitrate.

¹⁴ COM(2016) 790 final (8.12.2016).

¹⁵ COM(2018) 212 final (17.4.2018).

¹⁶ Regulation (EC) No 2252/2004 (OJ L 385, 29.12.2004, p.1).

5. *Improving controls on firearms import and export to prevent illegal firearms trafficking*

The Commission has taken a range of actions to restrict the supply of firearms available to criminals and terrorists. To complement action against firearms trafficking¹⁷ and the May 2017 revision of the Directive on the control of the acquisition and possession of firearms, the Commission adopted together with this Progress Report a **Recommendation**¹⁸ calling for immediate steps to improve the security of export, import and transit measures for firearms for civilian use, their parts and essential components and ammunition. The Recommendation calls for action on the part of EU Member States to **improve the traceability and security of export and import control procedures for firearms and the cooperation between authorities in the fight against firearms trafficking**. This Recommendation follows up on the December 2017 Commission report on the implementation of Regulation No 258/2012¹⁹ on firearms exports and imports. The report concluded that it is necessary to strengthen the system of export and import authorisations on firearms to control the conditions for legal trade and therefore better fight illegal firearm trafficking. The Commission will monitor the result of this Recommendation which will feed into the overall monitoring of the implementation of Regulation No 258/2012.

III. IMPLEMENTATION OF OTHER PRIORITY FILES ON SECURITY

1. *Countering terrorist content online*

As set out in the Commission Work Programme for 2018 and in previous Security Union Progress Reports, the Commission is promoting and stepping up cooperation with internet platforms to detect and remove terrorist and other illegal content online. On 1 March 2018, the Commission took another important step to tackle the urgent and serious issue of terrorist content online, with the adoption of a **Recommendation on measures to be taken by online service providers and Member States to enhance efforts in relation to illegal content online, including in particular terrorist content**.²⁰

Building on the September 2017 Communication on tackling illegal content online²¹, the Recommendation urges online service providers to ensure faster detection and removal of illegal content online, to reinforce co-operation between online service providers, trusted flaggers and EU law enforcement authorities, to increase the transparency of reporting to public authorities and to ensure safeguards for the fundamental rights of citizens. The Recommendation provides operational guidance to online service providers to take down terrorist content more quickly and to cooperate better with law enforcement. Given that terrorist content is typically most harmful in the first hour of its appearance online, and given the specific expertise and responsibilities of competent authorities and Europol, the Recommendation stresses that content identified in referrals should be assessed by online

¹⁷ See the EU action plan against illicit trafficking in and use of firearms and explosives (COM(2015) 624 final, 2.12.2015). Disrupting organised crime groups involved in the illicit trafficking, distribution and use of firearms is also a priority in the EU Policy Cycle for organised and serious international crime for the period 2018-2021.

¹⁸ C(2018) 2197.

¹⁹ Regulation No 258/2012 establishing export authorisation, and import and transit measures for firearms, their parts and components and ammunition.

²⁰ Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177 final).

²¹ Communication on Tackling illegal content online, towards enhanced responsibility of online platforms, COM 2017 (555) final (28.9.2017).

service providers and that, where appropriate, they should remove or disable access to it within one hour, as a general rule. It also recommends to platforms to be proactive and use automated tools to detect and identify terrorist content, and calls on them to use available technological tools to ensure that such content is not re-uploaded on other platforms.

A reporting exercise is now underway to allow for the monitoring of the effects given to the Recommendation. The information expected to be received from online service providers by early May 2018 will help the Commission decide whether the current approach is sufficient, or 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.

2. *Towards the interoperability of information systems and improved information exchange*

Working towards stronger and smarter information systems for security, border and migration management, the EU is addressing shortcomings in EU information management and sharing as a matter of urgency and as a top priority. All related legislative proposals are included in the Joint Declaration on the EU's legislative priorities for 2018-2019. Discussions between the co-legislators on the legislative proposals on the **interoperability** of EU information systems are advancing. Following the Justice and Home Affairs Council of 8 March 2018 where Member States expressed broad support for the interoperability components as proposed by the Commission, the Council aims to reach a general approach by June 2018. Technical discussions are also advancing swiftly at the European Parliament, with a view to entering into trilogue discussions with the co-legislators by July 2018 and reaching an agreement before the end of the year. For that, and as announced in December 2017²², it is necessary to present relevant amendments to the interoperability proposals relating to those legal instruments²³ that are currently under negotiations by the co-legislators. Given the shared objective of reaching agreement on the interoperability proposals before the end of 2018 as set out in the Joint Declaration on the EU's legislative priorities for 2018-19, this in turn **requires reaching swift agreement on those files that are still under negotiation**. In any case, the Commission will present, by mid-June 2018, all necessary amendments to its interoperability proposals to allow trilogues to commence by July 2018.

The interinstitutional negotiations on establishing a **European Travel Information and Authorisation System (ETIAS)** are in their final stages and the adoption should take place in the coming weeks.

Intensive work is undertaken to advance trilogue negotiations between the co-legislators on the three legislative proposals to strengthen the **Schengen Information System (SIS)**, in view of reaching a political agreement. The Commission calls on the co-legislators to reach agreement on the proposals by the end of May 2018. In parallel to this legislative work, the **Automated Fingerprint Search (AFIS)** functionality was launched on 5 March 2018 to strengthen the Schengen Information System in its current form. This technical improvement brings immediate and significant added-value to the work of border guards and law enforcement officers as it allows them to search the system by fingerprints to identify those

²² See the Twelfth progress report towards an effective and genuine Security Union (COM(2017) 779 final (12.12.2017)).

²³ The proposed Regulations on the European Travel Information and Authorisation System, the European Criminal Records Information System for third-country nationals, Eurodac, the Schengen Information System and eu-LISA.

entering or moving within the Schengen area. This constitutes a major milestone for security in the Schengen area as criminals using multiple or fraudulent identities will be more easily identified. As of this date, each newly created fingerprint record is checked against all existing SIS records to detect multiple identities. Moreover, the eleven Schengen States participating in the first phase of this project²⁴ now carry out searches with fingerprints. The new legal framework for SIS as proposed by the Commission, builds on the AFIS functionality, as it will provide for mandatory fingerprint checks if the identity of the person cannot be ascertained otherwise. The Commission calls on all remaining Member States to take the necessary steps to use the new functionality for primary checks at border crossings as well as for police checks within the territory. As another step to strengthen the use of the Schengen Information System, the Commission adopted together with this Progress Report a new version of the existing catalogue of recommendations and best practices emerging from Schengen evaluations in 2016 and 2017.

Trilogue negotiations between the co-legislators also continue on the proposals to facilitate the exchange of criminal records of third-country nationals in the EU through the **European Criminal Records Information System** and to strengthen the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (**eu-LISA**).

As part of the work to strengthen existing information systems and their interoperability, the Commission will present later in spring 2018, based on technical studies and an impact assessment, a proposal for the revision of the **Visa Information System** (VIS) to contribute to enhanced security at the external borders and within the Schengen area. The upcoming revision of the VIS legal framework will include specific interoperability measures to increase the efficiency of visa processing and is also planned to address other issues identified in the 2016 evaluation of the VIS.²⁵

The full implementation of the **Passenger Name Records** (PNR) Directive²⁶ is an essential part of parallel efforts to make full use of existing information systems, given the instrument's key role in the EU's common response to the threat of terrorism and serious cross border crime. Full implementation of the Directive by all Member States by the deadline of 25 May 2018 is imperative to allow full effectiveness at EU level. At the Justice and Home Affairs Council of 8 March 2018, those Member States which have not yet transposed the Directive emphasised that they were doing their utmost to meet the said deadline. As of 17 April 2018, five Member States²⁷ are still at a relatively early stage of the implementation process. The Commission once again urges these Member States to swiftly proceed with the transposition process and take every possible step to ensure that their Passenger Information Unit and PNR technical solution are operational within the remaining five weeks in order to meet the deadline of 25 May 2018.

The Commission continues encouraging and supporting all Member States in their efforts to implement the Directive, including with dedicated contacts at political and technical level with those five Member States. The eighth meeting on the implementation of the PNR Directive took place on 12 April 2018, which provided again an opportunity for the Member States and the Commission to address remaining implementation issues, as well as to start

²⁴ Austria, Germany, Latvia Liechtenstein, Luxembourg, Malta, the Netherlands, Poland, Portugal, Slovenia, Switzerland.

²⁵ Communication from the European Commission to the European Parliament and the Council: Adapting the common visa policy to new challenges (COM (2018) 251 final (14.3.2018)).

²⁶ Directive 2016/681 (27.4.2016).

²⁷ Croatia, Cyprus, Czech Republic, Greece and Italy.

looking into matters related to the application of the PNR Directive.

3. *Protection against chemical, biological, radiological and nuclear risks and the protection of public spaces*

The Salisbury chemical attack was a shocking reminder of the threat **chemical, biological, radiological and nuclear (CBRN) substances** can pose to security. As requested by the 22-23 March 2018 European Council, the EU must strengthen its resilience to CBRN risks in line with the Action Plan presented in October 2017.²⁸ The Action Plan set out a number of measures to reduce the accessibility of CBRN materials, address gaps in detecting such materials, and step up preparedness for and response to CBRN incidents. The measures also aim to foster cooperation against these threats in the EU and with key international partners, including NATO. This includes information exchange, joint capacity-building, training and exercises, including through cooperation with the NATO-accredited Joint CBRN Centre of Excellence in the Czech Republic. An EU CBRN Security Network is being established to pool all CBRN actors at both strategic and operational levels. It will bring together Member States, EU institutions, relevant Agencies and, where appropriate, key international partners and the private sector. Five Member States still need to nominate national CBRN Security Coordinators and should do so without delay. As requested by the European Council, the Commission and the High Representative will report on progress in the implementation of the CBRN Action Plan and in bolstering capabilities to address hybrid threats in view of the June 2018 European Council.

As part of implementing the Action Plan to support the **protection of public spaces**²⁹ notably against terrorist attacks, on 8 March 2018, the Commission and the European Committee of the Regions jointly organised the EU Mayors' Conference on "Building Urban Defences Against Terrorism: Lessons Learned From Recent Attacks" attended by almost 200 participants, including from cities recently hit by terrorist attacks. The conference focused on lessons learned from recent terrorist attacks, sharing of experiences and best practices. It allowed identifying solutions to enhance the physical protection of public spaces, while maintaining the openness and attractiveness of cities and public spaces, including the implementation of "security by design" concepts. EU funding is available under the Internal Security Fund to support the implementation of these solutions. The Commission currently assesses 35 project proposals it received under a related call. Later in 2018 a call under the Urban Innovative Actions with an overall budget of EUR 100 million from the European Regional Development Fund will also have security as one of its priorities. Security research also contributes to the overall efforts to strengthen the protection of public spaces. In 2019, a dedicated research topic on "Security for smart and safe cities, including for public spaces" with a budget of EUR 16 million will be launched.

4. *Cybersecurity*

Countering cybercrime and enhancing cybersecurity remains a priority for EU action. In order to create synergies, scale up existing competences and research and come up with marketable solutions that can improve cybersecurity of the Digital Single Market, the Commission launched, on 1 February 2018, a call for proposals for a EUR 50 million **pilot project to support the creation of a network of cybersecurity competence centres across the EU**. The network will bring together research expertise in cybersecurity from across the European

²⁸ COM(2017) 610 final (18.10.2017).

²⁹ Action Plan to support the protection of public spaces (COM(2017) 612 final (18.10.2017)).

Union (e.g. university labs/public or private non-profit research centres). This pilot project was announced in the Joint Communication on Cybersecurity³⁰ adopted September 2017 and funds will come from Horizon 2020 Framework Programme under the amended Work Programme 2018-2020. The deadline to respond to the call for proposals is 29 May 2018.³¹

The recent use of cyber means to manipulate behaviour, deepen societal divides and subvert democratic systems and institutions has only served to underscore the need to preserve tools which ensure accountability online. This was another aspect highlighted in the 2017 Joint Communication, notably by improving the **availability and accuracy of information in the "WHOIS" domain name registration database, which is** an important resource for cybercrime investigations and cybersecurity. As work is ongoing within ICANN to make this database compliant with data protection rules, in particular the General Data Protection Regulation, the Commission sent a letter³² to ICANN on the dual objectives of ensuring quick access to its directories for public interest purposes whilst being fully compliant with EU data protection rules. The ICANN Government Advisory Committee, in which national governments and the Commission are represented, voiced its concerns and called on ICANN to ensure continued access to the WHOIS, including non-public data, for users with a legitimate purpose.

In January 2018, the European Commission set up an independent High-Level Expert Group to advise on policy options to counter fake news and **disinformation** spread online and to help develop a comprehensive EU strategy in this regard. On 12 March 2018 the Group issued its report on "A Multi-dimensional approach to disinformation" that provides input for the Commission Communication on this issue planned to be adopted this spring.

On 16 April 2018, the **Foreign Affairs Council adopted Council conclusions on malicious cyber activities**. These conclusions are a practical implementation of the Joint EU Diplomatic Response to Malicious Cyber Activities (the "cyber diplomacy toolbox")³³ in response to specific malicious cyber activities, such as the *Wannacry* and *NotPetya* cyberattacks. The Foreign Affairs Council Conclusions underline the importance of an open, free, peaceful and secure cyberspace, and stress that the application of existing international law and the adherence to voluntary non-binding norms of responsible state behaviour are essential to maintaining peace and stability.

5. *External dimension*

To step up the collection and sharing of information to counter migrant smuggling, human trafficking, trafficking of firearms and trafficking of oil exports from Libya, the Justice and Home Affairs Council of 8-9 March 2018 endorsed the general principle of the participation of Europol and the European Border and Coast Guard Agency in a pilot project for a "**Crime Information Cell**" to be established within the EU's naval Common Security and Defence Policy Operation Sophia (EUNAVFOR MED). The Crime Information Cell will facilitate timely and two-way information exchange for analytical and operational use between Operation Sophia and the relevant Justice and Home Affairs Agencies. It is the first initiative

³⁰ JOIN(2017) 450 final (13.9.2017).

³¹ More information about the call is available on:
<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-ict-03-2018.html>.

³² <https://www.icann.org/resources/correspondence/1212685-2018-01-29-en>

³³ Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") of 19 June 2017.

of this kind between Justice and Home Affairs Agencies and the Common Security and Defence Policy missions or operations. The practical modalities are currently discussed in the Council in view of starting the pilot as soon as possible. Once launched, the project will be continuously evaluated with a full report to Member States after six months to assess the added value and performance of the Crime Information Cell as well as legal and operational aspects before any decision is taken on its continuation or replication in other Common Security and Defence Policy missions or operations.

Security in the **Western Balkans** directly impacts the security of the EU and its Member States. On 6 February 2018, the Commission adopted a Communication on A credible enlargement perspective for and enhanced EU engagement with the Western Balkans.³⁴ Its annexed Action Plan in Support of the Transformation of the Western Balkans sets out six thematic flagship initiatives, including on security and migration, to be completed by 2020. Work has started to implement a number of actions to step up cooperation with the Western Balkans to counter terrorism, prevent violent extremism and fight against organised crime, notably through the posting of Europol liaison officers across the region³⁵ and dedicated expert meetings with the participation of the Western Balkans such as the meeting of European firearms experts held in Sofia on 12-13 April 2018 and the EU Dialogue on Drugs in Brussels on 18 April 2018. The upcoming summit in Sofia on 17 May 2018 will also provide an opportunity to take stock of progress made in this regard.

IV. CONCLUSION

Six months after adopting a set of practical measures in October 2017 to better defend citizens in the EU against terrorist threats, the Commission presents together with this Progress Report a further set of measures to close down the space in which terrorists and criminals operate and to facilitate investigation and prosecution of crimes and terrorist attacks. The Commission invites the European Parliament and the Council to work on these legislative measures as a matter of urgency to enhance further the security of citizens.

Delivering a Europe that protects remains a political priority for the Union and the Commission will continue to work towards an effective and genuine Security Union, also in view of the informal meeting of Heads of State or Government on internal security as announced in the Leaders' Agenda for September 2018 in Vienna. The Commission will present the next Security Union Progress Report in June 2018.

³⁴ Commission Communication: A credible enlargement perspective for and enhanced EU engagement with the Western Balkans, (COM(2018) 65 final).

³⁵ By summer 2018, three Europol liaison officers will be posted in Albania, Bosnia Herzegovina and Serbia.