072710/EU XXVI. GP
Eingelangt am 26/07/19

Council of the
European Union

Brussels, 26 July 2019
(OR. en)

11501/19

JAI 845
COSI 159
FRONT 237
ASIM 89
DAPIX 248
ENFOPOL 354
SIRIS 120
VISA 164
FAUXDOC 55
COPEN 322
CYBER 232
DATAPROTECT 189
CT 79
JAIEX 113
EF 249

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	25 July 2019
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2019) 353 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Nineteenth Progress Report towards an effective and genuine Security Union

Delegations will find attached document COM(2019) 353 final.

Encl.: COM(2019) 353 final

EUROPEAN
COMMISSION

Brussels, 24.7.2019
COM(2019) 353 final

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

Nineteenth Progress Report towards an effective and genuine Security Union

www.parlament.gv.at

I. INTRODUCTION

This is the nineteenth report on the further 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.

Europeans rightly expect their Union to keep them safe. The Juncker Commission made security a top priority from day one. In the European Council's 'A new strategic agenda 2019-2024', the objective of 'protecting citizens and freedoms' ranks top of four main priorities for the Union.[1] The European Council further announced that it will build on and strengthen the Union's efforts in the fight against terrorism and cross-border crime, including through improving cooperation and information sharing and further developing common instruments.

Thanks to close cooperation between the European Parliament, the Council and the Commission, the EU has taken significant strides in the joint work towards an effective and genuine Security Union, putting in place a number of priority legislative initiatives and implementing a wide range of non-legislative measures to support its Member States and enhance security for all citizens.[2] The Union has taken decisive action to close down the space in which terrorists and criminals operate, denying terrorists the means to carry out attacks by prohibiting the acquisition and use of certain firearms and explosives and limiting the access to financing. The EU has also reinforced information sharing between Member States and closed information gaps and blind spots, while countering radicalisation, protecting Europeans online, tackling cyber and cyber-enabled threats, reinforcing the management of the Union's external borders, and strengthening international cooperation in the area of security.

At the same time, there are still a number of priority initiatives in the Security Union pending adoption by the co-legislators. Following the constitution of the 9th legislature of the European Parliament on 2 July 2019, this report:

- sets out where action is required by the co-legislators to address immediate threats. There is a particularly urgent need for action to **counter terrorist propaganda and radicalisation online**;
- sets out pending priority initiatives in the Security Union that require further action by the co-legislators to enhance **cybersecurity** and to facilitate the access to **electronic evidence** and to complete the work on stronger and smarter information systems for security, border and migration management;
- updates on the joint and urgent work launched in March 2019 to assess and strengthen **the security of 5G networks**, building on the national risk assessments that Member States submitted by 15 July 2019;
- addresses a package of four reports related to **anti-money laundering**, adopted by the Commission on 24 July 2019, that analyse the current risks and vulnerabilities in money laundering and assess how the relevant EU regulatory framework is being applied in the private and public sector;

[1] https://www.consilium.europa.eu/media/39914/a-new-strategic-agenda-2019-2024.pdf

[2] For an overview, see the factsheet on 'Security Union: A Europe that protects' (https://ec.europa.eu/commission/sites/beta-political/files/euco-sibiu-security-union_1.pdf) and the Eighteenth Progress Report towards an effective and genuine Security Union (COM(2019) 145 final, 20.3.2019).

- provides an update on the progress made since March 2019[3] in implementing legislative measures in the Security Union, with the interoperability of information systems being one of the top priorities for swift and complete implementation by Member States;
- takes stock of on-going work to counter disinformation and protect elections against cyber-enabled threats, efforts to enhance preparedness and protection against security threats, and the cooperation with international partners on security issues.

II. DELIVERING ON LEGISLATIVE PRIORITIES

1. Preventing radicalisation online and in communities

Preventing radicalisation is at the heart of the EU response to terrorism, both online and in our communities.

The horrific attack in Christchurch, New Zealand on 15 March 2019 served as an appalling reminder of how the internet can be harnessed for terrorist purposes, whether fuelled by jihadism, far right extremism or any other extremist ideology. The speed and scale at which the livestreamed Christchurch attack video spread across internet platforms highlighted the vital importance of internet platforms having adequate measures in place to stem the rapid propagation of such content.

In response, Heads of State or Government of some Member States and third countries, President Juncker and online platforms supported on 15 May 2019 the '**Christchurch Call to action**'[4] that sets out collective actions that aim to eliminate terrorist and violent extremist content online. Further commitments in that respect have been taken by the G7[5] and G20[6].

The Commission has already addressed the clear and present danger posed by terrorist content online with the **legislative proposal** that President Juncker announced in his 2018 State of the Union address, proposing a clear and harmonised legal framework to prevent the misuse of hosting service providers for the dissemination of terrorist content online.[7] The proposed measures would make it mandatory for internet platforms to take down terrorist content within one hour when they receive a removal order from competent authorities in any Member State. Additionally, if a platform is being abused to spread terrorist content, it would have an obligation to make use of proactive measures to detect this content and prevent it from reappearing – with clear rules and safeguards. Member State authorities would have to ensure dedicated law enforcement capacity with the resources to effectively detect terrorist content and issue removal orders.

[3] See the Eighteenth Progress Report towards an effective and genuine Security Union (COM(2019) 145 final, 20.3.2019).

[4] https://www.elysee.fr/emmanuel-macron/2019/05/15/the-christchurch-call-to-action-to-eliminate-terrorist-and-violent-extremist-content-online.en. French President Emmanuel Macron and New Zealand's Prime Minister Jacinda Ardern invited Leaders and online platforms to Paris on 15 May 2019 to launch this initiative.

[5] https://www.elysee.fr/en/g7/2019/04/06/g7-interior-ministers-meeting-what-are-the-outcomes

[6] At the G20 in Osaka on 28-29 June 2019, leaders reaffirmed their commitment to act to protect people from terrorist and violent extremism conducive to terrorism exploiting the internet (https://g20.org/pdf/documents/en/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf).

[7] COM(2018) 640 final (12.9.2018).

This will allow for a fast and effective Union-wide system, and will put robust safeguards in place, including effective complaint mechanisms and provision for judicial redress. The proposed measures will help guarantee the smooth functioning of the Digital Single Market, whilst increasing security and enhancing trust online and strengthening safeguards for freedom of expression and information.

In the Council, the Justice and Home Affairs Ministers agreed a general approach on the proposal in December 2018. The European Parliament adopted its position in first reading in April 2019. **The Commission calls on both co-legislators to enter into inter-institutional negotiations as quickly as possible on this priority initiative to remove terrorist content online**, with a view to reaching swift agreement on an EU regulatory framework with clear rules and safeguards.

In parallel, the Commission is continuing the cooperation with online platforms in the framework of the **EU Internet Forum**[8]. As announced by President Juncker at the Paris meeting on 15 May 2019 on the 'Christchurch Call to action', the Commission has, together with Europol, initiated work on the development of an **EU crisis protocol** to allow governments and internet platforms to respond rapidly and in a coordinated manner to the dissemination of terrorist content online, for instance in the immediate aftermath of a terrorist attack. This work is part of the efforts at international level to implement the 'Christchurch Call for Action'. In addition to further discussions with Member States and industry and a table top exercise planned for September 2019 to simulate an emergency situation, the Commission will convene an EU Internet Forum Ministerial meeting on 7 October 2019 with a view to endorsing the EU crisis protocol.

Moreover, the Commission is continuing its efforts to **support Member States and local actors in preventing and countering radicalisation** on the ground in local communities across Europe. This requires long-term, sustainable efforts involving all relevant actors at local, national and EU level. The **Steering Board for Union actions on preventing and countering radicalisation**, set up in August 2018 to advise the Commission on how to strengthen the EU policy response in this area, held its second meeting on 17 June 2019 to explore further actions in priority areas such as radicalisation in prisons and countering extremist ideologies. As frontline and grassroots practitioners are often best placed to identify early warning signs of radicalisation and ways to address them, the EU-funded **Radicalisation Awareness Network**[9] continues to support front-line responders, connecting around 5,000 practitioners from civil society, schools and police, as well as national coordinators and policy-makers.

Recent collaboration of front-line practitioners within the Network led to a deeper understanding of the challenges of far right extremism. This year the Radicalisation Awareness Network will publish fact sheets to help policy makers and practitioners to identify

[8] Launched in 2015, the **EU Internet Forum** brings together EU Home Affairs Ministers, the internet industry and other stakeholders to work together in a voluntary partnership to address the misuse of the internet by terrorist groups and to protect citizens.

[9] In 2011 the Commission established the **Radicalisation Awareness Network** to bring together frontline and grassroots practitioners. In 2015, the Commission strengthened the network by setting up the Radicalisation Awareness Network Centre of Excellence to develop more targeted guidance, support and counselling services to stakeholders in Member States and increase expertise and skills of different actors. For more information on the activities of the Radicalisation Awareness Network, see: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en.

the main forms and manifestations of far right and Islamist extremism, such as key narratives, language, forms, symbols, typologies and strategies. Finally, as local actors and **cities** are at the forefront in preventing and countering radicalisation, the Commission supports city-led initiatives on anti-radicalisation. Following up on a Conference on 'EU Cities against Radicalisation' on 26 February 2019, the first meeting of a pilot group of about 20 cities hosted by the Mayor of Strasbourg took place on 8 July 2019 to step up the exchange of best practices and enhance cities' efforts in this area.

In parallel, work is ongoing in supporting partner countries in addressing radicalisation that can lead to terrorism, including in prisons.

In order to counter the threat posed by terrorist content online, the Commission calls on the European Parliament and the Council:

- to enter into negotiations on the legislative proposal to prevent the dissemination of **terrorist content online**, with a view to reaching swift agreement on an EU regulatory framework with clear rules and safeguards.

2. *Enhancing cybersecurity*

Cybersecurity remains a key security challenge. The EU has made important progress[10] on tackling 'classic' cyber threats targeting systems and data, implementing the actions set out in the September 2017 Joint Communication[11] on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'. This inlcudes the EU Cybersecurity Act[12] that gives a permanent mandate to the European Union Agency for Cybersecurity, strengthening its role, and establishes an EU framework for cybersecurity certification. The Commission has also addressed sector-specific requirements, for example through its Recommendation on cybersecurity in the energy sector adopted on 3 April 2019.[13] But the continued increase in activity from malicious actors across a diverse range of targets and victims, means that efforts to counter cybercrime and enhance cybersecurity remain a priority for EU action.

The European Parliament and the Council still need to reach agreement on the Commission's priority initiative for a **European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres**.[14] The proposal aims to support cybersecurity technological and industrial capacities and to increase the competitiveness of the Union's cybersecurity industry. Both co-legislators adopted their negotiating mandates in March 2019. As it was not possible to conclude the inter-institutional negotiations before the end of the previous term of the European Parliament, the latter formally adopted its position in first reading. In the meantime, the discussions between Member States in the Council are continuing, with a particular focus on the interaction

[10] For more information, see the brochure on 'Building strong cybersecurity in the European Union: resilience, deterrence, defence': https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence.

[11] JOIN(2017) 450 final (13.9.2017).

[12] The EU Cybersecurity Act (Regulation (EU) 2019/881 of 17.4.2019) introduces, for the first time, EU wide rules for the cybersecurity certification of products, processes and services. In addition, the Cybersecurity Act sets a new permanent mandate for the EU Agency for Cybersecurity, as well as more resources allocated to the Agency to enable it to fulfil its goals. For more information on the call for proposals, see: https://ec.europa.eu/digital-single-market/en/news/eu10-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and-cross.

[13] C(2019) 2400 final (3.4.2019) and SWD(2019) 1240 final (3.4.2019).

[14] COM(2018) 630 final (12.9.2018).

between the proposed Regulation establishing the Cybersecurity Competence Centre and Network on the one side and the Horizon Europe and Digital Europe programmes on the other. **The Commission calls on both co-legislators to resume and swiftly conclude inter-institutional negotiations on this priority initiative to enhance cybersecurity.**

Meanwhile, the Commission continues to **support research and innovation** related to cybersecurity, making available EUR 135 million in the current multiannual financial framework for projects in areas such as cybersecurity in critical infrastructures, intelligent security and privacy management, and tools specifically for citizens and small and medium-sized enterprises.[15] In July 2019, the Commission issued a new call for proposals under the Connecting Europe Facility programme, making available EUR 10 million for EU funding to key actors identified by the Directive on the security of network and information systems (NIS Directive)[16] such as European Computer Security Incident Response Teams, operators of essential services (e.g. banks, hospitals, utility providers, railways, airlines, domain name providers) and various public authorities. For the first time, European cybersecurity certification authorities are also eligible to apply for this programme in order to allow them to implement the EU Cybersecurity Act.

On 17 May 2019, the Council adopted a **sanctions regime** which allows the EU to impose targeted restrictive measures to deter and respond to cyber-attacks constituting an external threat to the EU and its Member States. The new sanctions regime is part of the **EU's cyber diplomacy toolbox**[17], a framework for a joint EU diplomatic response to malicious cyber activities[18] that allows the EU to make full use of measures within the Common Foreign and Security Policy to deter and respond to malicious cyber activities.

Beyond cyber threats targeting systems and data, the EU is also taking action to address the complex and multifaceted challenges posed by **hybrid threats**.[19] The European Council, in its conclusions of 21 June 2019[20], underlined that *'the EU must ensure a coordinated response to hybrid and cyber threats and strengthen its cooperation with relevant international actors'*. The Commission welcomes that countering hybrid threats is also a priority of the Finnish Council Presidency and that a scenario-based policy discussion on hybrid threats was held at the 18-19 July 2019 informal meeting of Justice and Home Affairs Ministers in Helsinki. Similar scenario-based discussions on hybrid threats took place between EU defence policy directors on 7–8 July 2019 and between EU political directors on 9-10 July 2019, the outcome of which will be reported to foreign and defence ministers at a joint informal session on 29-30 August 2019.

[15] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/cross-cutting-activities-focus-areas

[16] Directive (EU) 2016/1148 (6.7.2016).

[17] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

[18] This includes cyber-attacks as well as attempted cyber-attacks with a potentially significant effect, involving e.g. access to information systems or data interception through digital infrastructure such as 5G networks (see also section III on enhancing security of digital infrastructures).

[19] See the report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats (SWD(2019) 200 final, 28.5.2019). See also the September 2016 legislative proposal for a Regulation setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast) (COM(2016) 616 final, 28.9.2016).

[20] https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf

In order to enhance cybersecurity, the Commission calls on the European Parliament and the Council:

- to reach swift agreement on the legislative proposal for a **European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres**.

3. Improving law enforcement access to electronic evidence

The EU has taken further action to deny terrorists and criminals the means to act, making it harder for them to access explosives precursors[21], finance their activities[22] and travel without detection[23].

Negotiations on the Commission's April 2018 proposals to improve law enforcement **access to electronic evidence** should be finalised as quickly as possible – more than half of all criminal investigations today involve a cross-border request to access electronic evidence.[24] The Council adopted its negotiating position on proposals for a Regulation[25] to improve the cross-border access to electronic evidence in criminal investigations and for a Directive[26] laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. Given the crucial importance of efficient access to electronic evidence for the investigation and prosecution of cross-border crimes such as terrorism or cybercrime, the Commission urges the European Parliament to advance on this proposal so that the co-legislators can work to swift adoption.

In parallel, the Commission is working on improving and ensuring necessary safeguards in **international exchange of electronic evidence** in the context of the ongoing negotiations of a Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime, as well as with the United States in line with the negotiating mandates given by the Council at the Justice and Home Affairs Council meeting on 6-7 June 2019.[27] The Commission participated in the latest round of negotiations on a Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime on 9-11 July 2019. The Commission and the United States authorities are currently preparing at technical level for the formal launch of the negotiations for an EU-U.S. Agreement on cross-border access to electronic evidence.

[21] Regulation (EU) 2019/1148 (20.6.2019) on the marketing and use of explosives precursors.

[22] Directive (EU) 2019/1153 (11.7.2019) laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences.

[23] Regulation (EU) 2019/1157 (20.6.2019) on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement.

[24] Electronic evidence is needed in around 85% of criminal investigations, and in two-thirds of these investigations there is a need to request evidence from online service providers based in another jurisdiction. See the Impact Assessment accompanying the legislative proposal (SWD(2018) 118 final (17.4.2018)).

[25] COM(2018) 225 final (17.4.2018). The Council adopted its negotiating mandate on the proposed Regulation at the Justice and Home Affairs Council on 7 December 2018.

[26] COM(2018) 226 final (17.4.2018). The Council adopted its negotiating position on the proposed Directive at the Justice and Home Affairs Council on 8 March 2019.

[27] https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

In order to improve law enforcement access to electronic evidence, the Commission calls on the European Parliament:

- to adopt its negotiating mandate on the legislative proposals on **electronic evidence** to enter swiftly into trilogue discussions with the Council. *(Joint Declaration priority)*

4. Stronger and smarter information systems for security, border and migration management

Following the adoption of rules on the **interoperability of information systems**[28], which will close information gaps and blind spots by helping to detect multiple identities and countering identity fraud, the Commission swiftly launched a series of initiatives to support Member States in the implementation process, including with funding where needed, as well as with workshops to facilitate the exchange of expertise and best practice. Close cooperation between EU Agencies, all Member States and Schengen associated countries will be paramount in order to achieve the ambitious objective of achieving full interoperability of EU information systems for security, border and migration management by 2020.

This objective also requires swift and complete implementation of recently agreed legislation to establish new information systems – the EU Entry/Exit System[29] and European Travel Information and Authorisation System[30] – as well as to reinforce the Schengen Information System[31] and to extend the European Criminal Records Information System[32] to third-country nationals. The new architecture for stronger and smarter information systems for security, border and migration management will only make a difference on the ground if all components are fully implemented at Union level and by each Member State, in accordance with the agreed timetable.

At the same time, there is need for further action by the co-legislators to complete the work on stronger and smarter information systems for security, border and migration management. As part of the technical implementation of the **European Travel Information and Authorisation System**, the Commission presented two proposals on 7 January 2019 setting out technical amendments to the related Regulation[33] that are necessary to fully set up the system. The Commission calls on the co-legislators to advance their work on these technical amendments in order to reach agreement as soon as possible, thus enabling swift and timely implementation of the European Travel Information and Authorisation System to make it operational in early 2021.

In May 2018, the Commission presented a proposal to **strengthen the existing Visa Information System**[34] providing for more thorough background checks on visa applicants and closing information gaps through better information exchange between Member States. The Council adopted its negotiating mandate on 19 December 2018, and on 13 March 2019 the European Parliament's Plenary voted its report on the proposal thus concluding its first reading. The Commission calls for a swift start of negotiations between the co-legislators under the newly constituted European Parliament.

[28] Regulation (EU) 2019/817 (20.5.2019) and Regulation (EU) 2019/818 (20.5.2019).

[29] Regulation (EU) 2017/2226 (30.11.2017).

[30] Regulation (EU) 2018/1240 (12.9.2018) and Regulation (EU) 2018/1241 (12.9.2018).

[31] Regulation (EU) 2018/1860 (28.11.2018), Regulation (EU) 2018/1861 (28.11.2018), Regulation (EU) 2018/1862 (28.11.2018).

[32] Regulation (EU) 2019/816 (17.4.2019).

[33] COM(2019)3 final and COM(2019) 4 final (7.1.2019).

[34] COM(2018) 302 final (16.5.2018).

In May 2016, the Commission proposed to extend the scope of **Eurodac**[35] by including not only the identification of asylum applicants but also that of illegally-staying third-country nationals and those who enter the EU irregularly. In line with the December 2018 European Council conclusions[36] and the Commission Communication of 6 March 2019 on progress in the implementation of the European Agenda on Migration,[37] the Commission calls on the co-legislators to proceed to the adoption of the proposal. It is necessary to adopt this legislative proposal in order to enable Eurodac to become part of the future architecture of interoperable EU information systems, thus integrating the crucial data of illegally staying third-country nationals and those who have entered the EU irregularly.

In order to strengthen the EU information systems for security, border and migration management, the Commission calls on the European Parliament and the Council:

- to adopt the legislative proposal on **Eurodac** *(Joint Declaration priority)*;
- to advance the work in view of reaching a swift agreement on the proposed technical amendments that are necessary to establish the **European Travel Information and Authorisation System.**

III. ENHANCING THE SECURITY OF DIGITAL INFRASTRUCTURES

The resilience of our digital infrastructure is critical to government, business, the security of our personal data and the functioning of our democratic institutions. The **fifth generation (5G) networks** which will be deployed in the coming years will form the digital backbone of our societies and economies, connecting billions of citizens, objects and systems, including in critical sectors such as energy, transport, banking, and health, as well as industrial control systems carrying sensitive information and supporting safety systems.

With worldwide revenues estimated to reach €225 billion in 2025, 5G is a key asset for Europe to compete in the global market and **the security of 5G networks is crucial for ensuring the strategic autonomy of the Union**. Ensuring a high level of cybersecurity requires concerted measures at both national and European level, as any vulnerability in 5G networks in one Member State would affect the Union as a whole.

Following the support from the Heads of State or Government expressed at the March 2019 European Council[38], the Commission presented on 26 March 2019 a **Recommendation on cybersecurity of 5G networks**[39], setting out actions to assess cybersecurity risks of 5G networks and to strengthen preventive measures. The recommendations build on coordinated EU risk assessment and risk management measures, an effective framework for cooperation and information exchange, and joint EU situational awareness covering critical communication networks.

As the **first stage** of the process initiated by the Recommendation, by 15 July 2019, all Member States had completed their **national risk assessment** and submitted their findings to the Commission and EU Agency for Cybersecurity, or have announced that they would do so

[35] COM(2016) 272 final (4.5.2016).

[36] https://www.consilium.europa.eu/en/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/

[37] COM(2019) 126 final (6.3.2019).

[38] https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/en/pdf

[39] C(2019) 2335 final (26.3.2019).

shortly. The national risk assessments followed a set of guidelines and a common template for reporting on findings agreed upon by Member States and the Commission in order to promote consistency and facilitate the exchange of information about national results at EU level. The parameters assessed in all Member States included:

- the main threats and threat actors affecting 5G networks;
- the degree of sensitivity of 5G network components and functions as well as other assets; and
- various types of vulnerabilities, including both technical otherwise, such as those potentially arising from the 5G supply chain.

In addition, the work on national risk assessments involved a range of responsible actors in the Member States such as, depending on the national responsibilities, authorities on cybersecurity, telecommunication, security and intelligence services, strengthening their cooperation and coordination. In parallel and in view of their national timetables for 5G deployment, a number of Member States have already taken steps to reinforce applicable security requirements in this area, while several others have indicated their intention to consider new measures in the near future.

Based on the results of the national risk assessment, Member States' cybersecurity authorities in the Network and Information Systems Cooperation Group[40] will prepare a **joint review of risks at EU level** by 1 October 2019, which will form the second stage of the process initiated under the Recommendation. Building on that, and as the third stage, the Cooperation Group will prepare a **common Union toolbox of mitigating measures** by 31 December 2019 to address the identified risks. The Commission and the EU Agency for Cybersecurity will continue to support the implementation of the Recommendation.

The work in the Network and Information Systems Cooperation Group is supported by several other fora. The Body of European Regulators for Electronic Communications is preparing a survey of all existing security measures that are potentially relevant for 5G. A new dedicated expert group in the EU Agency for Cybersecurity has launched work on the 5G Threat Landscape review. In addition, following the entry into force of the Cybersecurity Act on 27 June 2019, the Commission and the EU Agency for Cybersecurity will take all necessary steps to set up the EU-wide certification framework. Member States also met in the Standards Committee in June 2019 to discuss cybersecurity and standardisation in response to the Recommendation to explore future challenges for cybersecurity standardisation, including 5G networks, and suitable policy initiatives at the EU level.

Finally, the security of 5G networks is of strategic importance for the Union. Foreign investment in strategic sectors, acquisition of critical assets, technologies and infrastructure in the Union and supply of critical equipment may also pose risks to the Union's security.

[40] The Network Information Security Cooperation Group is set up under Directive EU) 2016/1148 (6.7.2016) on the security of network and information systems. As envisaged in the Recommendation, a dedicated work stream within the Network Information Security Cooperation Group was set up, led by several Member States. The group has already met thrice – in April, May and July 2019 - to share information about national approaches and to discuss how to facilitate the preparation of the EU coordinated risk assessment.

The new **EU framework for the screening of foreign direct investments**[41] entered into force on 10 April 2019. Over the next 18 months, the Commission and Member States will take the necessary steps to make sure that the EU can fully apply the Investment Screening Regulation as of 11 October 2020.

IV. ANTI-MONEY LAUNDERING

The ability of criminals and terrorists to transfer funds between bank accounts in a matter of hours enables them to more easily prepare their acts of terror or to illegally launder the proceeds of crime, across different Member States. To address this challenge, the Union has developed a solid **regulatory framework for countering money laundering and terrorist financing**, in line with international standards adopted by the Financial Action Task Force.

Given the need to keep pace with evolving trends, technological developments and the adapting ingenuity of criminals to exploit any gaps or loopholes in the system, on 24 July 2019, the Commission adopted a **package of four reports** that analyse the current risks and vulnerabilities related to money laundering, and assess the way the framework is applied by the relevant actors both in the private and public sector.[42]

The package includes an **assessment of the potential interconnection of national centralised bank account registries and data retrieval systems** in the EU. Such national centralised systems allow the identification of any natural or legal person holding or controlling payments accounts, bank accounts and safe deposit boxes – information that is often crucial for competent authorities in the fight against money laundering and terrorist financing. The 5th Anti-Money Laundering Directive[43] requires Member States to put in place such national centralised systems and provide their national Financial Intelligence Units with direct access. The recently adopted rules to facilitate the use of financial information to counter serious crime[44] provide designated law enforcement authorities and Asset Recovery Offices with direct access to their respective national centralised bank account registries. Building on that, and as required under the Anti-Money Laundering Directive, the report assesses various IT solutions at EU level, already operational or under development, which may serve as a model for a possible interconnection of the national centralised systems. Given that a future EU-wide interconnection of the centralised mechanisms would speed up access to financial information and facilitate the cross-border cooperation of the competent authorities, the Commission intends to further consult with the relevant stakeholders,

[41] Regulation (EU) 2019/452 (19.3.2019) establishing a framework for the screening of foreign direct investments into the Union. The new framework creates a cooperation mechanism where Member States and the Commission will be able to exchange information and raise concerns related to specific investments. It will also allow the Commission to issue opinions when an investment poses a threat to the security or public order of more than one Member State, or when an investment could undermine a project or programme of interest to the whole EU. The Member State where the investment takes place has the final word on how to treat the investment.

[42] Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (COM (2019) 370 final of 24.7.2019), Report on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts (COM(2019) 372 final of 24.7.2019), Report on the assessment of recent alleged money laundering cases involving EU credit institutions (COM(2019) 373 final of 24.7.2019), Report assessing the framework for cooperation between Financial Intelligence Units (COM(2019) 371 final of 24.7.2019).

[43] Directive (EU) 2015/849 (20.5.2015).

[44] Directive (EU) 2019/1153 (20.6.2019).

governments, as well as the Financial Intelligence Units, law enforcement authorities and Asset Recovery Offices, as potential 'end-users' of a possible interconnection system.

As part of the Commission's reflection on the work of Financial Intelligence Units, a report assessing the **cooperation between Financial Intelligence Units** looks both at cooperation within the Union and with third countries.[45] It identifies certain shortcomings which are likely to continue to exist until the tasks and cross-border cooperation obligations of Financial Intelligence Units are more clearly spelled out in the EU legal framework for anti-money laundering and countering terrorist financing. The assessment also shows a need for a stronger mechanism to coordinate and support cross-border cooperation and analysis.

Looking beyond the existing work to tackle money laundering and terrorist financing, and also in response to a call by the European Parliament,[46] the Commission will continue to assess the necessity, technical feasibility and proportionality of additional measures to track terrorist financing in the EU.[47]

V. IMPLEMENTATION OF OTHER PRIORITY FILES ON SECURITY

1. Implementation of legislative measures in the Security Union

Reaching agreement on measures under the Security Union is not the end of the process – it is vital to subsequently ensure their swift and complete implementation by Member States so that the full benefits can be enjoyed. To this end, the Commission is actively supporting Member States, including through funding and by facilitating the exchange of best practices. Where necessary, however, the Commission stands ready to make full use of its powers under the Treaties for the enforcement of EU law, including infringement action when appropriate.

The deadline for the implementation of the **EU Passenger Name Record Directive**[48] passed on 25 May 2018. To date, 25 Member States have notified full transposition to the Commission.[49] Full transposition is still absent in two Member States, despite the infringement procedures launched on 19 July 2018.[50] In parallel, the Commission continues to support all Member States in their efforts to complete the development of their passenger name record systems, including by facilitating the exchange of information and best practices.

The deadline for transposition of the **Directive on combating terrorism**[51] passed on 8 September 2018. To date, 22 Member States have notified full transposition to the Commission. Three Member States still fail to communicate the adoption of national legislation which fully transposes the Directive, despite the infringement procedures launched

[45] This assessment is required by Article 65(2) of the 5th Anti-Money Laundering Directive (EU) 2018/843 (30.5.2018).

[46] In its final report adopted in December 2018, the European Parliament's Special Committee on Terrorism called for the establishment of a European Union Terrorist Financing Tracking System targeted on transactions by individuals with links to terrorism and their financing within the Single Euro Payments Area.

[47] See the Eighteenth Progress Report towards an effective and genuine Security Union (COM(2019) 145 final, 20.3.2019).

[48] Directive (EU) 2016/681 (27.4.2016).

[49] The references to complete transposition notification take account of the Member States' declarations and are without prejudice to the transposition check by the Commission services.

[50] Slovenia notified partial transposition. Spain did not notify transposition (state of play as of 24 July 2019).

[51] Directive (EU) 2017/541 (15.3.2017).

on 22 November 2018.[52]

The deadline for transposition of the **Directive on the control of the acquisition and possession of weapons**[53] passed on 14 September 2018. To date, 8 Member States have notified full transposition to the Commission. 20 Member States still fail to communicate the adoption of national measures which fully transpose the Directive, despite the infringement procedures launched on 22 November 2018.[54]

With respect to the transposition into national law of the **Data Protection Law Enforcement Directive**[55], the deadline for transposition passed on 6 May 2018. To date, 20 Member States have notified full transposition to the Commission.[56] 7 Member States still fail to communicate the adoption of national measures which fully transpose the Directive, despite the infringement procedures the Commission launched on 19 July 2018.[57]

Member States had until 9 May 2018 to transpose the **Directive on the security of network and information systems**[58] into national law. To date, 26 Member States have notified full transposition to the Commission and 2 Member States have partially transposed the Directive.[59] Moreover, by 9 November 2018, Member States were required to identify operators of essential services in line with the Directive. By 9 May 2019, the Commission was supposed to submit a report to the European Parliament and the Council assessing the consistency of the approach in the identification of operators of essential services identified within their territory. However, as a number of Member States had yet to submit complete information on the identification process, the Commission has had to delay its report.

The Commission is assessing the transposition of the **4th Anti-Money Laundering Directive**[60], while also working to verify that the rules are implemented by Member States. The Commission is engaged in infringement procedures against 24 Member States as it assessed that the communications received from the Member States do not represent a complete transposition of this Directive.[61]

The Commission calls on Member States, as a matter of urgency, to take the necessary measures to fully transpose the following Directives into national law and communicate them to the Commission:

[52] Poland notified partial transposition. Greece and Luxemburg did not notify transposition (state of play as of 24 July 2019).

[53] Directive (EU) 2017/853 (17.5.2017).

[54] Belgium, Czechia, Estonia, Lithuania, Poland, Portugal, Sweden and the United Kingdom notified partial transposition. Germany, Ireland, Greece, Spain, Cyprus, Luxembourg, Hungary, Netherlands, Romania, Slovenia, Slovakia and Finland did not notify transposition (state of play as of 24 July 2019).

[55] Directive (EU) 2016/680 (27.4.2016).

[56] 20 Member States completed the transposition (state of play as of 24 July 2019).

[57] Latvia, Portugal, Slovenia and Finland notified partial transposition. Greece and Spain did not notify transposition. Although Germany notified complete transposition, the Commission considers this transposition not to be complete (state of play as of 24 July 2019).

[58] Directive (EU) 2016/1148 (27.4.2016).

[59] Belgium and Hungary partially transposed the Directive (state of play as of 24 July 2019).

[60] Directive (EU) 2015/849 (20.5.2015).

[61] Belgium, Bulgaria, Czechia, Denmark, Germany, Estonia, Ireland, Spain, France, Italy, Cyprus, Latvia, Lithuania, Hungary, Netherlands, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Finland, Sweden and the United Kingdom (state of play as of 24 July 2019).

- the **EU Passenger Name Record Directive**, where 1 Member State still needs to notify transposition into national law and 1 Member State needs to complete the notification of transposition;[62]
- the **Directive on combating terrorism**, where 2 Member States still need to notify transposition into national law and 1 Member State needs to complete the notification of transposition;[63]
- the **Directive on the control of the acquisition and possession of weapons**, where 12 Member States still need to notify transposition into national law and 8 Member States need to complete the notification of transposition;[64]
- the **Data Protection Law Enforcement Directive**, where 2 Member States still need to notify transposition into national law and 5 Member States need to complete the notification of transposition;[65]
- the **Directive on security of network information systems**, where 2 Member States still need to complete the notification of transposition;[66] and
- the **4th Anti-Money Laundering Directive**, where 24 Member States still need to complete the notification of transposition.[67]

2. Countering disinformation and protecting elections against other cyber-enabled threats

Protecting democratic processes and institutions from disinformation and related interference is a major challenge for societies across the globe. To tackle this, the EU has put in place a **robust framework for coordinated action against disinformation**, with full respect for European values and fundamental rights.[68] As set out in the Joint Communication of 14 June 2019 on the implementation of the Action Plan against Disinformation[69], the work on several complementary strands has helped close down the space for disinformation and preserve the integrity of the European Parliament elections.

The European Council, in its conclusions of 21 June 2019[70], welcomed the Commission's intention to conduct an in-depth evaluation of the implementation of commitments undertaken by online platforms and other signatories under the **Code of Practice against**

[62] Slovenia notified partial transposition. Spain did not notify transposition (state of play as of 24 July 2019).

[63] Poland notified partial transposition. Greece and Luxemburg did not notify transposition (state of play as of 24 July 2019).

[64] Belgium, Czechia, Estonia, Lithuania, Poland, Portugal, Sweden and the United Kingdom notified partial transposition. Germany, Ireland, Greece, Spain, Cyprus, Luxembourg, Hungary, Netherlands, Romania, Slovenia, Slovakia and Finland did not notify transposition (state of play as of 24 July 2019).

[65] Latvia, Portugal, Slovenia and Finland notified partial transposition. Greece and Spain did not notify transposition. Although Germany notified complete transposition, the Commission considers this transposition not to be complete (state of play as of 24 July 2019).

[66] Belgium and Hungary partially transposed the Directive (state of play as of 24 July 2019).

[67] Belgium, Bulgaria, Czechia, Denmark, Germany, Estonia, Ireland, Spain, France, Italy, Cyprus, Latvia, Lithuania, Hungary, Netherlands, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Finland, Sweden and the United Kingdom (state of play as of 24 July 2019).

[68] See the Action Plan against Disinformation (JOIN(2018) 36 final of 5.12.2018).

[69] JOIN (2019) 12 final (14.6.2019).

[70] https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf. The European Council's call builds on input by the Romanian Council Presidency as well as the Commission and the High Representative for Foreign Affairs and Security Policy on lessons learnt with regard to disinformation and securing free and fair elections, including the Joint Communication on the implementation of the Action Plan against Disinformation.

Disinformation[71] and invited the Commission and the High Representative of the Union for Foreign Affairs and Security Policy to continuously assess and appropriately respond to the *"evolving nature of the threats and the growing risk of malicious interference and online manipulation associated with the development of Artificial Intelligence and data-gathering techniques"*.

The Commission and the High Representative will advance its work in this area in line with the European Council's conclusions. In March 2019, the Commission and the High Representative set up a **Rapid Alert System** among the EU institutions and Member States to facilitate the sharing of insights related to disinformation campaigns and coordinate responses. The first meeting of Member States' contact points following the European Parliament elections took place in Tallinn on 3-4 June 2019. To further strengthen the Rapid Alert System, the High Representative and the Commission, in close cooperation with Member States, will review the functioning of the Rapid Alert System in autumn 2019. They will also develop a common methodology for the analysis and exposure of disinformation campaigns as well as stronger partnerships with international partners such as the G7 and NATO.

Work also continues in the **European Cooperation Network on Elections**[72] which held a first meeting on 7 June 2019 to take stock of the elections to the European Parliament. These reflections and further input from relevant national authorities, political parties and online platforms will contribute to the Commission's comprehensive report on the European Parliament elections to be adopted in October 2019. Member States have used the network with regards to elections other than those to the European Parliament, which highlights its broader usefulness for securing the integrity of democracy in the EU.

The Commission will also continue to monitor and promote the implementation of the commitments undertaken by platforms in the **Code of Practice against Disinformation**. The reports provided by Google, Twitter and Facebook under the Code of Practice show that all the platforms took action in advance of the European Parliament elections by labelling political ads and making them publicly available via searchable ad libraries. At the same time, there is room for improvement as identified by the European Regulators Group for Audiovisual Media Services.[73] Notably, there is still a lack of access to the detailed raw data necessary for comprehensive monitoring. Finally, platforms should give the research

[71] The Code of Practice was signed by the online platforms Facebook, Google and Twitter, Mozilla, as well as by advertisers and advertising industry in October 2018 and sets self-regulatory standards to fight disinformation. The Code aims at achieving the objectives set out by the April 2018 Commission Communication on tackling online disinformation (COM/2018/236 final of 26.4.2018) by setting a wide range of commitments, from transparency in political advertising to the closure of fake accounts and demonetization of purveyors of disinformation.

[72] The European Cooperation Network on Elections brings together the contact points of national election cooperation networks of authorities with competence for electoral matters and authorities in charge of monitoring and enforcing rules related to online activities relevant to the electoral context. The European Cooperation Network on Elections serves to alert on threats, exchange on best practices among national networks, discuss common solutions to identified challenges and encourage common projects and exercises among national networks.

[73] The European Regulators Group for Audiovisual Media Services brings together heads or high level representatives of national independent regulatory bodies in the field of audiovisual services to advise the Commission on the implementation of the EU's Audiovisual Media Services Directive (Directive 2010/13/EU of 10.3.2010). At its latest meeting on 20-21 June 2019 in Bratislava, the Group presented the outcomes of the work done so far on disinformation, with a focus on the 2019 European Parliament elections and the related areas of political and issue-based advertising.

community meaningful access to data, in line with personal data protection rules. Later this year, the Commission will conduct a comprehensive assessment of the implementation of all commitments under the Code of Practice during its initial 12-month period. On this basis, the Commission may consider further actions, including of a regulatory nature, to improve the long-term EU's response to disinformation.

3. *Preparedness and protection*

Strengthening defences and building resilience against security threats is an important aspect of the work towards an effective and genuine Security Union. This includes the support the Commission provides to Member States and their local authorities to reinforce the **protection of public spaces**[74], as well as the support to Member States in enhancing preparedness against **chemical, biological, radiological and nuclear security risks**[75], implementing the two action plans in this area, as well as analysing the needs for related response capacities to be developed under rescEU[76]. As regards evolving chemical threats,[77] in cooperation with Member States and in consultation with international partners, the Commission has developed a list of chemicals that are of most concern in terms of misuse for terrorist purposes. The EU list serves as the basis for further work to reduce accessibility to these chemicals, and to work with manufacturers on improving detection capabilities.

Technologies for unmanned aircraft allow a wide range of possible operations. With a rapid expansion over recent years in the market in unmanned aircraft systems for military, civilian commercial and hobby purposes, **drones** represent an opportunity but also an increasing security threat to critical infrastructure (including aviation), public spaces and events, sensitive sites and individuals. In Europe, drones have been used to disrupt aviation and law enforcement operations, to survey critical infrastructure and to smuggle contraband into prisons and over borders.

The Commission supports Member States in countering the growing threat posed by drones to citizens and critical societal functions without discarding their beneficial use e.g. in emergency response operations. The Commission recently adopted **common EU-wide rules on the safe operation of drones**[78] to mitigate the risk of their malicious use, which include provisions requiring operator registration and enabling remote identification. Moreover, the Commission supports Member States by monitoring trends in the evolution of the threat posed by drones, funding relevant research projects and capacity-building measures, and

[74] See the 'Good practices for public authorities and private operators to strengthen the security of public spaces', as set out in the Eighteenth Progress Report towards an effective and genuine Security Union (COM(2019) 145 final of 20.3.2019). This builds on the October 2017 Action Plan to support the protection of public spaces (COM(2017) 612 final of 18.10.2017). On 5 June 2019, the third meeting of the Operators' Forum of the EU Forum on the protection of public spaces took place. It has brought together representatives of the EU Member States and private operators of public spaces, represented through 14 European associations, covering the hospitality sector, live performances, music and entertainment, amusement parks and attractions, the aviation, railway transport, shopping centres, telecommunication, as well as the private security services and the security equipment manufacturers.

[75] Notably by implementing the October 2017 Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks (COM(2017) 610 final of 18.10.2017).

[76] See Article 12(2) of Decision No 1313/2013/EU on the Union Civil Protection Mechanism (17.12.2013), as amended by Decision (EU) 2019/420 (13.3.2019).

[77] See the reinforced actions against chemical threats as set out in the Fifteenth Progress Report towards an effective and genuine Security Union (COM(2018) 470 final of 13.6.2018).

[78] OJ L 152, 11.6.2019 - Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.

facilitating exchange between Member States and other stakeholders. To step up this support, the Commission will organise a high-level international conference on 17 October 2019 to counter the risks posed by drones.

In response to a need to take a broad view on EU policy on **critical infrastructure protection**[79], the Commission presented on 23 July 2019 an evaluation of the European Critical Infrastructure Directive[80] as the legal framework for the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. The evaluation found that the context in which critical infrastructures in Europe operate has changed considerably since the Directive entered into force, including with legislative developments in sectors particularly targeted by the Directive such as energy[81], and that the provisions of the Directive are only partially relevant as a result of the evolved landscape. At the same time, there is continued support from Member States for EU policy on critical infrastructure protection that respects subsidiarity and provides added value.

4. External dimension

Given the cross-border and global nature of most security threats facing our Union, cooperation with international organisations and partner countries outside the EU is an integral part of the work towards an effective and genuine Security Union.

Leveraging the benefits of multilateral cooperation is an integral part of this effort, and includes the cooperation between the EU and the UN, as recently reinforced with the signing of the **framework on counter-terrorism between the UN and the EU** in New York on 24 April 2019, on the occasion of the second UN-EU high-level political dialogue on counter-terrorism.[82] The framework promotes cooperation on capacity building to counter terrorism and prevent and counter violent extremism in Africa, the Middle East and Asia. The framework identifies areas for UN-EU cooperation and priorities until 2020.

The **security cooperation with the Western Balkans** represents a particular regional priority, implementing a number of security-related priority actions identified in the 2018 Western Balkans Strategy.[83] To that end, on 4 April 2019 the Commission organised the first meeting of the Inter-Agency Task Force for the Western Balkans, where representatives of seven EU agencies shared their experience and enhanced operational cooperation with partners in the region, including in the fight against organised crime, terrorism, firearms, drugs, migrant smuggling and trafficking in human beings. Hybrid risk surveys have been launched with all six Western Balkan countries. Another tangible example of the cooperation with the region is the European Border and Coast Guard Status Agreement between the EU and Albania that entered into force on 1 May 2019, which was swiftly followed by a deployment of the European Border and Coast Guard Agency teams to the border with Greece. This is the first such agreement with and deployment to a third country. Similar

[79] The 2017 Comprehensive Assessment of EU Security Policy (SWD(2017) 278 final, 26.7.2017) pointed to a need to take a broad view on EU critical infrastructure protection policy.

[80] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection aims to enhance the protection of critical infrastructure in the European Union.

[81] In particular Regulation (EU) 2017/1938 (25.10.2017) concerning measures to safeguard the security of gas supply and Regulation (EU) 2019/941 (5.6.2019) on risk preparedness in the electricity sector.

[82] https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf

[83] COM(2018) 65 final (6.2.2018).

agreements should soon be signed with other countries in the region.

In addition, a Europol liaison officer was deployed in Albania in July 2019 to further assist the Albanian authorities in their efforts to prevent and combat organised crime. To step up the fight against firearms trafficking, the Commission presented on 27 June 2019 an evaluation of the 2015-2019 Action Plan **countering firearms trafficking** between the EU and the South-eastern region of Europe.[84] The evaluation demonstrates the added-value of cooperation but highlights that further effort is still required, e.g. by putting in place efficient national coordination centres on firearms or by harmonising the collection of information and reporting on firearm seizures.

Equal priority is given by the EU to developing **cooperation with Middle Eastern and North African countries** in the area of security. The EU has launched a Security dialogue with Tunisia and Algeria. The EU and Tunisia held the 3rd dialogue on Security and Counter-Terrorism on 12 June in Tunis, whereas the 2nd dialogue EU-Algeria on Security and Counter-Terrorism took place on 12 November 2018 in Algiers. Talks are ongoing to launch a structured Security dialogue with Morocco, following the recent Association Council of 27 June, where the EU and Morocco recognised the importance of deepening cooperation on security to face common challenges. In parallel, discussions are ongoing to develop a structured security dialogue with Egypt, as also further confirmed by the last Senior Official meeting EU-Egypt held on 10 July in Cairo.

Based on the mandate from the Council, the Commission has started informal talks with most **Middle Eastern and North African** countries in view of launching formal negotiations for an international agreement for the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (**Europol**) and the relevant competent authorities in **Middle Eastern and North African** countries for fighting serious crime and terrorism. Within this context, the Commission is also promoting the conclusion of working arrangements directly between Europol and partner authorities in the **Middle Eastern and North African** countries, to provide a formal framework for regular strategic-level cooperation.

The EU and the **United States** are close and strategic partners in addressing common threats and enhancing security. At their Justice and Home Affairs Ministerial Meeting on 19 June 2019, the EU and the United States reaffirmed that fighting terrorism is among their top priorities. As regards the EU-US Passenger Name Record Agreement[85], both parties reiterated the importance of the agreement and committed to begin a joint evaluation in September 2019 to assess its implementation, in line with the provisions of the agreement. Both parties also committed to enhance their joint efforts in fighting terrorism, including by expanding the sharing of information gathered in zones of combat for use in investigations and prosecutions.

To step up this cooperation, the Commission, together with the EU Counter-Terrorism Coordinator, hosted a high-level workshop on battlefield information on 10 July 2019 in Brussels. It brought together senior officials from Member States' ministries of defence, home affairs and justice, the United States, Europol, Eurojust and representatives of international organisations to exchange views on the use of battlefield information and reflect together on

[84] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190627_com-2019-293-commission-report_en.pdf

[85] OJ L 215, 11.8.2012, p. 5.

the procedural, legal and operational challenges that they currently face in seeking to identify terrorists and bring them to justice. The EU and the United States also held a Chemical, Biological, Radiological and Nuclear Capacity Building Dialogue in Brussels on 14-15 May 2019 to coordinate efforts in reducing threats from weapons of mass destruction and strengthening CBRN security globally.

The **Terrorist Financing Tracking Programme agreement between the EU and the United States**[86] is in place since 2010 and it regulates the transfer and processing of data for the purpose of identifying, tracking and pursuing terrorists and their networks. The agreement contains guarantees that ensure the protection of EU citizens' data and foresees a regular review of 'the safeguards, controls, and reciprocity provisions'. In a regular evaluation report[87] published on 22 July 2019, the Commission noted that it is satisfied that the Agreement, including its essential safeguards and controls, is being properly implemented. It welcomes the continued transparency of the United States authorities in sharing information, thereby illustrating the value of the Terrorist Financing Tracking Programme in our joint counterterrorism efforts. The information provided under the Agreement has been instrumental in bringing forward specific investigations relating to terrorist attacks on European soil, including the attacks in Stockholm, Barcelona and Turku in 2017. Member States and Europol have increased their use of the mechanism, and Terrorist Financing Tracking Programme data has generated seven times more investigative leads than in the previous reporting period. The next Joint Review of the agreement is expected in 2021.

As regards international cooperation on the exchange of **Passenger Name Records for the purposes of fighting terrorism and serious crime**, at the 17th EU-Canada Summit in Montreal on 17-18 July 2019, the EU and Canada welcomed that they have concluded negotiations for a new Passenger Name Record Agreement. While Canada noted its requirement for legal review, the parties commit, subject to that review, to finalising the Agreement as soon as possible, acknowledging the vital role of this Agreement in enhancing security while ensuring privacy and the protection of personal data. As regards the existing EU-Australia Passenger Name Records Agreement[88], a visit of an EU team to Canberra will take place in August 2019 in the context of the Joint Review and Joint Evaluation of the agreement.

The Commission is also working with Member States in the Council on an EU position for the upcoming 40th Session of the **International Civil Aviation Organisation** Assembly that will take place from 24 September to 4 October 2019. The Assembly will set out political direction and provide instructions to the International Civil Aviation Organisation Council on the technical work on International Civil Aviation Organisation standards for the processing of Passenger Name Record data. The Council endorsed an information paper prepared by the Commission to outline the Union's position on the core principles that should underpin any future global Passenger Name Records standard. The information paper will be put before the body in respect of its members other than EU Member States.

VI. CONCLUSION

Thanks to close cooperation between the European Parliament, the Council, the Member

[86] OJ L 195, 27.7. 2010, p. 5.
[87] COM(2019) 342 final (22.7.2019).
[88] OJ L 186, 14.7.2012, p. 4.

States and the Commission, the EU has made considerable progress over recent years in the joint work towards an effective and genuine Security Union, agreeing on a number of priority legislative initiatives. Member States, with the support of the Commission, are also implementing a variety of non-legislative operational measures to enhance security for all citizens. At the same time, there are still a number of pending priority initiatives in the Security Union that require further action by the co-legislators to address immediate threats. The Commission calls on the European Parliament and the Council to take the necessary steps to reach swift agreement on the legislative proposals to counter terrorist propaganda and radicalisation online, to enhance cybersecurity, to facilitate the access to electronic evidence and to complete the work on stronger and smarter information systems for security, border and migration management.

The Commission calls on Member States to implement swiftly and completely all legislation adopted in the Security Union to ensure its full benefits. Moreover, the Commission calls on Member States to continue and step up the crucial work on practical measures to enhance the security of digital infrastructures, to counter disinformation and other cyber-enabled threats, to step up preparedness and protection, and to reinforce the cooperation with partners outside the Union against shared threats. Taken together, these measures enhance collectively the security of all citizens.