



Council of the
European Union

038418/EU XXVI. GP
Eingelangt am 15/10/18

Brussels, 15 October 2018
(OR. en)

13094/18

JAI 998
COSI 220
FRONT 326
ASIM 125
DAPIX 311
ENFOPOL 495
SIRIS 134
VISA 269
FAUXDOC 92
COPEN 345
CYBER 230
DATAPROTECT 214
CT 160
JAIEX 134
EF 250

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	11 October 2018
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union

No. Cion doc.:	COM(2018) 690 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Sixteenth Progress Report towards an effective and genuine Security Union

Delegations will find attached document COM(2018) 690 final.

Encl.: COM(2018) 690 final

13094/18

MP/dk

JAI.1

EN



Brussels, 10.10.2018
COM(2018) 690 final

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

Sixteenth Progress Report towards an effective and genuine Security Union

I. INTRODUCTION

Security is the top concern of our citizens. Europeans rightly expect to be kept safe. The Union has an important role to play in enhancing internal security and in addressing citizens' concerns. In his **2018 State of the Union address**¹, European Commission President Jean-Claude Juncker underlined that only a strong and united Europe can protect citizens against threats, both internal and external, including from terrorism. Over the past few years, the European security landscape has been modernised with new legislation and policy initiatives in the Security Union, reinforced cooperation between Member States and a strengthened role for Union Agencies, particularly Europol and the European Border and Coast Guard Agency. In his address, President Juncker also called for leadership in completing the Security Union to meet citizens' expectations on internal security.

On the occasion of the 2018 State of the Union, the Commission presented a number of **measures to strengthen security** in the EU and to reinforce the protection of the EU's external borders. The Commission presented new rules to get terrorist content taken swiftly off the web, combining clear and targeted rules to prevent online services from being misused to disseminate terrorist content while ensuring strong safeguards to protect freedom of speech and information in an open and democratic society.² The Commission proposed measures to help ensure that next year's elections to the European Parliament are organised in a free, fair and secure manner, including a Recommendation on election cooperation networks, online transparency, protection against cybersecurity attacks and fighting disinformation campaigns.³ To keep pace with the ever-evolving cyber threat, the Commission proposed a Regulation to pool resources and expertise in cyber technology through the creation of a Network of Cybersecurity Competence Centres.⁴ As part of a comprehensive response to cross-border terrorist threats, the Commission put forward an initiative to extend, over time, the competences of the European Public Prosecutor's Office (EPPO) to terrorist crimes affecting more than one Member State.⁵ Finally, the Commission also proposed to strengthen the protection of the external borders by extending the competences of the European Border and Coast Guard and by reinforcing its capacity to act.⁶

The Commission presented these proposals as a contribution to the **Leaders' Meeting in Salzburg** on 19-20 September 2018, which served to highlight the need to focus on European solutions to reinforce Member States' capacities to deal with constant and evolving threats. As we approach the European Parliament elections, it is imperative that we deliver on the shared objective of enhancing the security of all citizens in the EU. The discussion in Salzburg therefore provided an opportunity to give positive momentum for the adoption of priority legislative initiatives before the European Parliament elections in May 2019, including the latest initiatives put forward by the Commission with the 2018 State of the Union. The coming months will be decisive to advance as far as possible on pending legislative proposals so as to conclude inter-institutional negotiations during this term of the European Parliament.

¹ https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_en_0.pdf. See also President Juncker's Letter of Intent: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-letter-of-intent_en.pdf.

² COM(2018) 640 final (12.9.2018).

³ COM(2018) 637 final (12.9.2018).

⁴ COM(2018) 630 final (12.9.2018).

⁵ COM(2018) 641 final (12.9.2018).

⁶ COM(2018) 631 final (12.9.2018).

Greater impetus must be given to delivering on the initiatives in the Security Union to enhance our collective security and resilience against cyber threats, which undermine the international rules-based system. On 4 October 2018 it was announced⁷ that the offices of the Organisation for the Prohibition of Chemical Weapons in The Hague had been, in April 2018, the target of a hostile cyber operation carried out by the Russian military intelligence service. This operation was disrupted by Dutch intelligence services in partnership with the United Kingdom. The President of the European Council Donald Tusk, the President of the European Commission Jean-Claude Juncker and High Representative/Vice-President Federica Mogherini jointly expressed serious concerns about this attempt to undermine the integrity of the Organisation for the Prohibition of Chemical Weapons and deplored such actions.⁸ The EU must all the more continue to strengthen the resilience of its institutions and those of its Member States, as well as international partners and organisations, in the digital domain. This further highlights the importance of the actions in the Security Union, supporting Member States in addressing the threats posed by cyber and cyber-enabled attacks, hybrid threats and chemical, biological, radiological and nuclear (CBRN) risks.

This sixteenth Security Union progress report sets out the overall state of play, highlighting the latest Commission initiatives accompanying the 2018 State of the Union address and progress made since the last report⁹ in June 2018, including on the **legislative priorities** agreed between the Presidents of the European Parliament, the Council and the Commission in their Joint Declaration of 14 December 2017 (see also the list of all initiatives in the Security Union in Annex I).¹⁰

II. DELIVERING ON LEGISLATIVE PRIORITIES

Agreement has been reached over the last months on a number of legislative priorities in the Security Union: the co-legislators reached agreement on the proposal to establish a European Travel Information and Authorisation System (ETIAS) that will allow for advance security and irregular migration checks of persons travelling visa-free to the EU;¹¹ they agreed to strengthen the Schengen Information System, the most widely used information sharing system for security and border management in Europe;¹² they reached agreement on the proposal to reinforce the mandate of eu-LISA, the EU Agency for the operational management of large-scale IT systems in the area of freedom, security and justice;¹³ they agreed on stronger rules criminalising money laundering;¹⁴ and they adopted new measures to strengthen EU rules to prevent money laundering and terrorist financing with the 5th Anti-Money Laundering Directive.¹⁵ For those measures which have not yet been adopted, this final step should be taken swiftly.

For a large number of proposals, agreement is still pending and further efforts are needed.

⁷ <https://english.defensie.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw>.

⁸ http://europa.eu/rapid/press-release_STATEMENT-18-6026_en.htm.

⁹ COM(2018) 470 final (13.6.2018).

¹⁰ https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-eu-legislative-priorities-2018-19_en.pdf.

¹¹ COM(2016) 731 final (16.11.2016).

¹² COM(2016) 881 final (21.12.2016), COM(2016) 882 final (21.12.2016), COM(2016) 883 final (21.12.2016).

¹³ COM(2017) 352 final (29.6.2017).

¹⁴ COM(2016) 826 final (21.12.2016).

¹⁵ Directive (EU) 2018/843 (30.5.2018).

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

To ensure that Member States' law enforcement officers and border guards have complete, accurate and reliable information, when and where they need it, in December 2017 the Commission put forward legislative proposals to establish the **interoperability of EU information systems** for security, border and migration management, and amended these proposals in June 2018.¹⁶ The proposed measures will allow national authorities to detect multiple identities and counter identity fraud. The Council obtained a negotiating mandate on 14 June 2018, which was supplemented on 12 September 2018 with regards to the consequential amendments. The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) is expected to vote on its negotiating mandate in the coming days, and the subsequent confirmation of the mandate by the European Parliament's Plenary is planned for the week of 22 October 2018. All three institutions agreed in the Joint Declaration to ensure delivery of the proposed Regulations on interoperability before the European Parliament elections of 2019. To achieve this it is necessary to stick to an ambitious timetable as foreseen by the co-legislators.

Negotiations on the legislative proposal¹⁷ to extend the **European Criminal Records Information System** to third-country nationals – another legislative priority in the area of information sharing – are in the final phase. The proposal foresees establishing a centralised database that will make it possible to quickly verify if any Member State holds conviction information on a non-EU citizen. Final agreement on the file is within reach, and the next trilogue meeting, planned for 17 October 2018, should allow the co-legislators to conclude the discussions on this priority legislative initiative in line with the Joint Declaration.

As regards the Commission's proposal¹⁸ to strengthen **Eurodac** by expanding its remit to include not only the identification of asylum applicants but also that of illegally-staying third-country nationals and those who enter the EU irregularly, there has been no progress in negotiations over the past months, despite the preliminary political agreement reached between the co-legislators in June 2018. There is an urgent need for the co-legislators to finalise this priority legislative initiative in line with the agreement under the Joint Declaration. This is necessary, on the one hand, to ensure that data on illegally staying third-country nationals and those who have entered the EU irregularly is part of the proposed interoperability of EU information systems, and on the other hand, as part of an effort to find a swift solution on the asylum reform. The proposal to strengthen Eurodac is one of the five most advanced files aimed at reforming the Common European Asylum System; like with the other advanced files the co-legislators should conclude negotiations before the end of 2018.

¹⁶ COM(2017) 793 final (12.12.2017), COM(2017) 794 final (12.12.2017), COM(2018) 478 final (13.6.2018), COM(2018) 480 final (13.6.2018).

¹⁷ COM(2017) 344 final (29.6.2017).

¹⁸ COM(2016) 272 final (4.5.2016).

Additionally, work is ongoing in the European Parliament and the Council on the May 2018 legislative proposal¹⁹ to strengthen the **Visa Information System (VIS)**. The proposal provides for enlarging the scope of the database to include data on long stay documents and their holders, enhanced checks across databases to detect and identify potential migration and security risks before visas are issued or upon issuance of a long stay document, and for strengthened capacity to prevent, detect and investigate crime. The Commission calls on the European Parliament and the Council to adopt their negotiating mandate by the end of 2018 and enter into trilogue discussions in early 2019 at the latest, as this will be necessary to allow the co-legislators to reach agreement on this file during the current term of the European Parliament.

To achieve stronger and smarter information systems for security, border and migration management, the Commission calls on the European Parliament and the Council:

Joint Declaration priorities:

- to enter into trilogue discussions in October 2018 on the legislative proposals on **interoperability**, and to reach an agreement by the end of the year;
- to reach agreement in October 2018 on the legislative proposal to extend the **European Criminal Records Information System** to third-country nationals;
- to finalise negotiations on the legislative proposal on **Eurodac** by the end of 2018.

Other:

- to adopt their negotiating mandate by the end of 2018 on the legislative proposal to strengthen the **Visa Information System**.

2. *Strengthening security through enhanced external border management*

Internal security is dependent on reinforced protection of the external borders. On 12 September 2018, on the occasion of the 2018 State of the Union address, the Commission adopted legislative proposals²⁰ to **strengthen the mandate of the European Border and Coast Guard** as well as that of the **European Union Agency for Asylum**²¹ and to reinforce **returns**.²² Taken together these proposals will provide for the necessary tools to better ensure the effective management of migration at the external borders.

The Commission proposed a number of changes to the European Border and Coast Guard Agency, in particular by providing it with its own operational arm: a European Border and Coast Guard standing corps of 10,000 operational staff with executive powers by 2020, for all its activities to effectively support Member States on the ground through reliable and readily available support. It will ensure that the European Border and Coast Guard Agency has the necessary capabilities, including its own equipment, to protect the EU external borders, prevent secondary movements and effectively implement returns of irregular migrants.

¹⁹ COM(2018) 302 final (16.5.2018).

²⁰ COM(2018) 631 final (12.9.2018).

²¹ COM(2018) 633 final (12.9.2018).

²² COM(2018) 634 final (12.9.2018).

The proposal will also reinforce cooperation with third countries and will further enhance the possibilities for the exchange of information between the Agency and Europol, including personal data related to suspects of cross-border crime. This proposal is a **clear priority** for the Commission, and it calls on the European Parliament and the Council to adopt the proposed legislation during the current term of the European Parliament. For this to happen, both co-legislators should adopt their negotiating mandate by the end of 2018 at the latest, for trilogue discussions to start early in 2019.

To strengthen security through enhanced external border management, the Commission calls on the European Parliament and the Council:

2018 State of the Union initiatives:

- to adopt by the end of 2018 their negotiating mandate on the legislative proposals to strengthen the **European Border and Coast Guard** and the **European Union Agency for Asylum** as well as the legislative proposal on the **Return Directive**, in order to adopt the legislation during the current term of the European Parliament.

3. Preventing radicalisation

Addressing **terrorist content online** remains a key challenge in fighting terrorism and preventing radicalisation. Recent terrorist attacks on EU soil have demonstrated how terrorists consistently and systematically misuse the internet to groom and recruit supporters, to prepare and facilitate terrorist activity, to glorify their atrocities and urge others to follow suit, and to instil fear in the general public. Hosting service providers, responding to calls from public authorities, have put in place certain measures to tackle terrorist content on their platforms through voluntary frameworks and partnerships, including the EU Internet Forum, launched in December 2015. However, there is a need to enhance action on the part of hosting service providers and Member States in relation to terrorist content online.

To tackle this serious problem, and in response to urgent calls by the European Parliament²³ and the European Council²⁴, President Juncker's 2018 State of the Union address was accompanied by a **legislative proposal** to establish a clear and harmonised legal framework to prevent the misuse of hosting service providers for the dissemination of terrorist content online.²⁵ The proposal builds on the March 2018 Commission Recommendation²⁶ 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.

²³ The European Parliament, in its resolution on online platforms and the digital single market of 15 June 2017, urged the platforms concerned "to strengthen measures to tackle illegal and harmful content", and called on the Commission to present proposals to address these issues.

²⁴ The European Council of 22-23 June 2017 called for industry to "develop new technology and tools to improve the automatic detection and removal of content that incites to terrorist acts. This should be complemented by the relevant legislative measures at EU level, if necessary". The European Council of 28 June 2018 welcomed "the intention of the Commission to present a legislative proposal to improve the detection and removal of content that incites hatred and to commit terrorist acts".

²⁵ COM(2018) 640 final (12.9.2018).

²⁶ C(2018) 1177 final (1.3.2018).

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. Member States' competent authorities will be able to issue removal orders obliging hosting service providers to remove terrorist content online within one hour, which is the point at which terrorist content is most harmful because of the speed at which it is disseminated. Under the proposal, Member States will need to ensure that their competent authorities have the necessary capacity to intervene against terrorist content online. The proposal will also provide clarity as to the responsibility of hosting service providers to take all appropriate, reasonable and proportionate actions necessary to ensure the safety of their services and to swiftly and effectively detect and remove terrorist content online, taking into account the fundamental importance of the freedom of expression and information in an open and democratic society. It also introduces a number of necessary safeguards designed to ensure full respect for fundamental rights such as freedom of expression and information in an open and democratic society, in addition to the possibility for judicial redress guaranteed by the right to an effective remedy.

This proposal is a **clear priority** for the Commission, and it calls on the European Parliament and the Council to adopt the proposed legislation during the current term of the European Parliament. For this to happen, both co-legislators should adopt their negotiating mandate by the end of 2018 at the latest, for trilogue discussions to start early in 2019.

In parallel to the legislative work to counter terrorist content online, the Commission will continue to work with hosting service providers within the voluntary framework of the **EU Internet Forum** to reduce accessibility to terrorist content online and empower civil society partners to increase the volume of effective alternative narratives online. It will be convened again at Ministerial level in December 2018.

At the same time, the EU continues to support the **prevention of radicalisation in Member States and their local communities**. On 1 and 2 October 2018, the EU Network of Prevent Policy Makers met to start implementing the recommendations of the High-Level Expert Group on Radicalisation.²⁷ This will feed into the work of the newly established Steering Board for Union actions on preventing and countering radicalisation that will convene for the first time in Vienna on 24 October 2018.²⁸ On 11 October 2018, the 4th Radicalisation Awareness Network (RAN) High-Level Conference on Radicalisation will bring together Ministers and practitioners to address the challenges posed by children returning from terrorist-held territory (including child refugees) as well as challenges around the release of radicalised detainees including terrorist offenders from prison. As part of the 2018 work programme of the Internal Security Fund²⁹ for police cooperation and crime prevention, providing total funding of EUR 70 million, the Commission will launch a call for proposals for targeted funding of EUR 5 million for preventing and countering radicalisation.

²⁷ See the Fifteenth Progress Report towards an effective and genuine Security Union (COM(2018) 470 final (13.6.2018)).

²⁸ C(2018) 5345 (9.8.2018).

²⁹ C(2018) 6336 (4.10.2018).

To prevent radicalisation, the Commission calls on the European Parliament and the Council:

2018 State of the Union initiative:

- to adopt by the end of 2018 their negotiating mandate on the legislative proposal to prevent the dissemination of **terrorist content online**, in order to adopt the legislation during the current term of the European Parliament.

4. Addressing cyber-enabled threats and enhancing cybersecurity

Ensuring the resilience of our democracies is a crucial part of the Security Union: attacks against electoral infrastructure and campaign information systems are hybrid threats that the Union urgently needs to address. Politically motivated mass online disinformation campaigns, including those perpetrated by third countries with the specific aim of discrediting and delegitimising elections, have been recognised as a growing threat to our democracies.³⁰ To address these complex threats, the Commission has been taking a number of initiatives, ranging from measures against cyber incidents aimed at reinforcing the Union's cybersecurity, to actions aimed at tackling online disinformation and manipulation, including through misuse of personal data.

Most recently, as announced by President Juncker in his 2018 State of the Union address, the Commission put forward a set of measures on 12 September 2018 for **securing free and fair European elections**.³¹ With a **Recommendation** on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns, the Commission is encouraging Member States to set up a national election cooperation network of relevant authorities – such as electoral, cybersecurity, data protection and law enforcement authorities – and to appoint a contact point to participate in a European-level election cooperation network.³² Also, Member States need to check whether their election laws are prepared for the reality of online campaigning. They also need to ensure that electoral rules and sanctions which apply to offline activities, including on transparency and campaign financing, can be enforced for online activities. The Commission calls on Member States as well as European and national political parties, foundations and campaign organisations to implement the actions set out in the Recommendation as a matter of urgency.

³⁰ JOIN(2018)16 final (12.6.2018).

³¹ COM(2018) 637 final (12.9.2018).

³² C(2018) 5949 final (12.9.2018).

Moreover, the Commission put forward **guidance on the application of EU data protection law** that will help national authorities and European and national political parties and other actors involved in the electoral process to apply the data protection obligations under EU law in the electoral context.³³ The Commission also presented a **legislative proposal for a targeted change of the 2014 Regulation on party funding** that will make it possible to impose financial sanctions for breaching data protection rules with the aim of deliberately influencing the outcome of the European elections.³⁴ Sanctions will consist of fines up to 5% of the annual budget of the European political party or foundation concerned. This proposal is a clear priority for the Commission, and it urges the European Parliament and the Council to ensure that the proposed targeted changes are in place in time for the 2019 elections to the European Parliament. For this to happen, both co-legislators should adopt their negotiating mandate as a matter of urgency, for trilogue discussions to start without delay.

Through the implementation of the European approach for **tackling online disinformation** as set out in April 2018³⁵, the Commission is promoting a more transparent, trustworthy and accountable online environment. On 26 September 2018, online platforms and the advertising industry unveiled a self-regulatory **Code of Practice on Online Disinformation** that includes a wide range of commitments to fight online disinformation. The Commission will closely follow the progress made and will analyse and report on the first results of the Code of Practice by the end of 2018.

The Commission will raise awareness and continue its dialogue with Member States' authorities, notably through the high-level conference on cyber-enabled threats to elections to be held on 15-16 October 2018, the outcome of which will feed into the next Colloquium on Fundamental Rights (26-27 November 2018), focused on "Democracy in the European Union". The analysis of the results of the Code of practice and the conclusions of the high-level conference will feed into a **joint action plan to fight disinformation** that the Commission and the High Representative will present by the end of the year, as a follow-up to the European Council conclusions of June 2018 and the 2018 State of the Union address. This action plan will report on progress made in implementing the Communication on tackling online disinformation. Building on the experience of the East Stratcom Task Force³⁶, the action plan will submit proposals to promote a more joined-up approach to disinformation in close cooperation with Member States.³⁷ The action plan will also look at the mandate and resources of the three Task Forces and consider ways of strengthening their capacity to address disinformation originating in the three regions. This will help ensure that efforts at EU and Member States levels are sufficiently scaled to address the complexity of disinformation campaigns conducted by hostile actors.

³³ COM(2018) 638 final (12.9.2018).

³⁴ COM(2018) 636 final (12.9.2018).

³⁵ COM(2018) 236 final (26.4.2018). In the Communication on Tackling online disinformation: a European Approach, the Commission put forward actions and requested to step up self-regulatory tools to tackle the spread and impact of online disinformation in Europe.

³⁶ The East Stratcom Task Force was set up to address Russia's ongoing disinformation campaigns, following the June 2015 Action Plan on Strategic Communication. The Task Force develops communication products and campaigns focused on better explaining EU policies. Two other task forces have been created with different geographic focus: the Western Balkans Stratcom Task Force and the South Med Stratcom Task Force for the Arab-speaking world.

³⁷ See also the Joint Communication on Increasing resilience and bolstering capabilities to address hybrid threats (JOIN(2018)16 final (12.6.2018)).

Countering cybercrime and enhancing cybersecurity also remain a priority for the EU. On 12 September 2018, as part of the 2018 State of the Union the Commission adopted a legislative proposal for a Regulation³⁸ to **pool resources and expertise in cybersecurity technology**. To keep up with the ever-evolving cyber threat, the proposal will create a **Network of National Coordination Centres** to better target and coordinate available funding for cybersecurity cooperation, research and innovation. A new European Industrial, Technology and Research Cybersecurity Competence Centre will manage EU financial resources dedicated to cybersecurity under the proposed Digital Europe Programme and Horizon Europe Programme and facilitate joint investment by the Union, Member States and industry to boost the EU's cybersecurity industry. Moreover, under the future European Defence Fund, recently proposed by the Commission, it will be possible, in principle, to support cyber defence projects. The European Industrial, Technology and Research Cybersecurity Competence Centre could act as a project manager for such projects, if requested by Member States. This proposal is a clear priority for the Commission, and it calls on the European Parliament and the Council to adopt the proposed legislation during the current term of the European Parliament. For this to happen, both co-legislators should adopt their negotiating mandate by the end of 2018 at the latest, for trilogue discussions to start early in 2019.

As part of the actions set out in the September 2017 Joint Communication³⁹ on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", the co-legislators held two trilogue meetings on 13 September 2018 and 1 October 2018 on the proposed **Cybersecurity Act**.⁴⁰ In order to increase cybersecurity capabilities and the preparedness of Member States and businesses, as well as to improve cooperation and coordination across Member States and EU institutions, agencies and bodies, the proposal will renew the mandate of the EU Agency for Network and Information Security and rename it as EU Cybersecurity Agency. The proposal will also establish an EU cybersecurity certification framework for information and communications technology products, systems and services. All three Institutions have reconfirmed their commitment to finalise the negotiations on the proposal before the end of year, in line with the Joint Declaration.

There has also been progress on the legislative proposal on **non-cash means of payment**, another part of the September 2017 Cybersecurity Package.⁴¹ The proposed rules will update the EU's legal framework against fraud and counterfeiting of non-cash means of payment, addressing new challenges and technological developments such as virtual currencies and mobile payments, removing obstacles to operational cooperation and enhancing prevention measures and assistance for victims. The co-legislators held a first trilogue meeting on 26 September 2018, and all three Institutions have indicated their willingness to reach a swift agreement on the proposal.

³⁸ COM(2018) 630 final (12.9.2018).

³⁹ JOIN(2017) 450 final (13.9.2017).

⁴⁰ COM(2017) 477 final (13.9.2017).

⁴¹ COM(2017) 489 final (13.9.2017).

To address cyber-enabled threats and enhance cybersecurity, the Commission calls on the European Parliament and the Council:

2018 State of the Union initiatives:

- to ensure that the proposed **targeted changes of the Regulation on party funding** are in place in time for the 2019 elections to the European Parliament;
- to adopt by the end of 2018 their negotiating mandate on the legislative proposal on the **European Industrial, Technology and Research Cybersecurity Competence Centre** and the **Network of National Coordination Centres**, in order to adopt the legislation during the current term of the European Parliament.

Joint Declaration priority:

- to reach agreement before the end of the year on the the proposed **Cybersecurity Act**.

Other:

- to reach agreement on the legislative proposal on **non-cash means of payment** during the current term of the European Parliament.

5. Closing down the space in which terrorists operate

The EU has taken **firm action** to close down the space in which terrorists and other criminals operate. Systematic security checks for all persons crossing the external border⁴² and the processing of data under the Passenger Name Record Directive⁴³ make it harder for terrorists to enter and move around the EU. The Directive on combating terrorism⁴⁴ helps to prevent terrorist attacks by criminalising acts such as the financing of terrorism, undertaking training or travelling for terrorist purposes, as well as organising or facilitating such travel. Strengthened rules to prevent money laundering and terrorist financing under the 5th Anti-Money Laundering Directive⁴⁵, as well as recently agreed rules to counter money laundering by criminal law⁴⁶, will make it more difficult for terrorists to get access to money. The Commission calls on Member States to transpose these instruments as rapidly as possible to step up the fight against terrorist financing and money laundering. The strengthened legal framework on the control of the acquisition and possession of weapons⁴⁷, together with continued action against firearms trafficking⁴⁸, restricts the supply of firearms available to criminals and terrorists.

⁴² Regulation (EU) 2017/458 (15.3.2017).

⁴³ Directive (EU) 2016/681 (27.4.2016).

⁴⁴ Directive (EU) 2017/541 (15.3.2017).

⁴⁵ Directive (EU) 2018/843 (30.5.2018).

⁴⁶ COM(2016) 826 final (21.12.2016).

⁴⁷ Directive (EU) 2017/853 (17.5.2017).

⁴⁸ 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. In April 2018, the Commission adopted a Recommendation for Member States to reinforce the implementation of the rules on the export and import of civilian firearms notably by carrying out systematic background checks on all individuals applying for export authorisations (C(2018) 2197 final).

While significant progress is being made to address terrorism and other security threats in the EU, there is no common Union approach to the investigation, prosecution and sentencing of cross-border terrorist crimes. Being the only Union body with the power to conduct criminal investigations and prosecute criminal offences before the competent national courts and bring the perpetrators to justice, the European Public Prosecutor's Office (EPPO)⁴⁹ holds great potential to substantially enhance the current efforts in the fight against terrorist crimes in the European Union. As a follow up to the 2017 State of the Union address, the Commission presented on 12 September 2018 an initiative to **extend the competence of the EPPO to investigate and prosecute cross-border terrorist offences**, together with a draft European Council Decision amending Article 86 TFEU with regard to the competences of the EPPO.⁵⁰ The Commission invites the European Council to take this initiative forward together with the European Parliament and to decide on the extension of the competences of the EPPO to terrorist offences affecting more than one Member State.

While the EU has strong anti-money laundering rules in place, recent cases involving money laundering in some EU banks have raised concerns that those rules are not always supervised and enforced effectively across the EU. On 12 September 2018, as part of the 2018 State of the Union, the Commission proposed to **reinforce the role of the European Banking Authority in anti-money laundering supervision of the financial sector**.⁵¹ The proposed measures will further strengthen the supervision of EU financial institutions to better address money-laundering and terrorist financing threats. The Commission calls on the European Parliament and Council to endorse the proposed actions to reinforce the role of the European Banking Authority and to adopt the relevant legislative measures as soon as possible and by early 2019 at the latest.

Electronic evidence is important in a large majority of criminal investigations. Increasingly often, judicial authorities need to make a request in another jurisdiction in order to obtain such electronic evidence data from service providers. Making it easier and quicker to obtain this evidence, including across borders, is of crucial importance for investigating and prosecuting crime, including terrorism or cybercrime, in an effective manner. There is therefore a real need for the co-legislators to adopt the April 2018 Commission proposals to improve the cross-border gathering of **electronic evidence** for criminal proceedings.⁵² In the Council, discussions are ongoing. The upcoming Justice and Home Affairs Council meeting from 11-12 October 2018 is an important occasion for Ministers to discuss key aspects of the proposals, notably on the scope of the initiative as well as its procedural aspects and necessary safeguards, with a view to agreeing on the Council's position by December 2018 at the latest. Given the importance of electronic evidence for criminal investigations in almost all types of crime, the Commission calls on the European Parliament and the Council to work on this priority legislative initiative as a matter of urgency, adopt their negotiating mandate by the end of 2018 at the latest, and enter into trilogue discussions without delay. This would still allow delivery of this legislative act before the European elections of 2019, as agreed by all three Institutions in the Joint Declaration.

⁴⁹ Council Regulation (EU) 2017/1939 (12.10.2017).

⁵⁰ COM(2018) 641 final (12.9.2018).

⁵¹ COM(2018) 645 final (12.9.2018).

⁵² COM(2018) 225 final (17.4.2018) and COM(2018) 226 final (17.4.2018).

The Commission continues to follow closely the **developments on electronic evidence in non-EU countries**, including the United States' Clarifying Lawful Overseas Use of Data Act (CLOUD Act), and it will be discussed at political level at the EU-US Justice and Home Affairs Ministerial Meeting in Washington on 8-9 November 2018. The Commission is also closely following developments on the negotiation of a Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime on access to electronic evidence. The Commission's proposals on electronic evidence provide a solid basis for a coordinated and coherent approach both within the EU, and by the EU at international level. The Commission intends to propose as soon as possible the adoption of two recommendations for negotiating directives on the international aspects of the e-evidence proposals as called for by the Justice and Home Affairs Council in June 2018, namely on the Budapest Cybercrime Convention's Second Additional Protocol and on an agreement between the EU and the United States on cross-border access to electronic evidence. The timing of the adoption of the two recommendations, which would be done jointly, is related to the progress made in the discussions on the e-evidence proposals and to sufficient clarity about the parameters and safeguards of the future EU internal arrangements as well as the safeguards needed in the legal systems of third-country partners.

Given the importance of financial information for investigations, the Commission presented in April 2018 a legislative proposal to **facilitate the use of financial and other information** for the prevention, detection, investigation or prosecution of serious criminal offences.⁵³ This priority legislative initiative seeks to provide designated law enforcement authorities and Asset Recovery Offices with direct access to bank account information held in national centralised bank account registries, and to strengthen cooperation between national Financial Intelligence Units and law enforcement authorities. The Commission calls on the European Parliament and the Council to work on the priority legislative initiative as a matter of urgency, given the agreement by all three Institutions in the Joint Declaration on Legislative Priorities to ensure delivery of this legislative act before the European Parliament elections of 2019. This requires that both co-legislators adopt their negotiating mandate as a matter of urgency and enter into trilogue discussions without delay.

Terrorists have used homemade explosives in many attacks in the EU, and an even higher number of failed and foiled attacks involved the attempted use of homemade explosives. To restrict as much as possible terrorists' access to dangerous explosives precursors that can be misused to make homemade explosives, in April 2018 the Commission put forward a legislative proposal to strengthen the **restrictions on the marketing and use of explosives precursors**.⁵⁴ Building on a the Commission Recommendation⁵⁵ of October 2017, this initiative seeks to close security gaps with a number of measures such as banning additional chemicals which could be used to make homemade explosives, mandatory checks of the criminal records of those who apply for a licence for the purchase of restricted substances, and clarifying that rules applicable to economic operators also apply to companies that operate online. To reach these objectives, it is important that the co-legislators adopt their negotiating mandate by the end of 2018 and enter into trilogue negotiations in early 2019 at the latest, as only this will allow the co-legislators to reach agreement on this file during the current term of the European Parliament.

⁵³ COM(2018) 213 final (17.4.2018).

⁵⁴ COM(2018) 209 final (17.4.2018).

⁵⁵ C(2017) 6950 final (18.10.2017).

To make it more difficult for terrorists and other criminals to misuse or falsify documents used to enter or move around the EU while facilitating the exercise of EU citizens' free movement rights, the Commission presented in April 2018 a legislative proposal to enhance the **security features of national identity cards and residence documents**.⁵⁶ The proposal sets out minimum document security standards for national identity cards, including in particular the need for a biometric photo and fingerprints to be stored in a chip on the identity card. The proposal also outlines the minimum information to be provided on residence documents issued to EU citizens living in another Member State, as well as full harmonisation of the format of the residence cards of non-EU family members. Both co-legislators are expected to obtain their negotiating mandate by November 2018, which should provide a basis for swift progress and adoption of the file during the current term of the European Parliament.

To close down the space in which terrorists operate, the Commission invites the European Council:

2018 State of the Union initiative:

- to take forward the initiative to extend the competence of the **European Public Prosecutor's Office**.

The Commission also calls on the European Parliament and the Council:

2018 State of the Union initiative:

- to endorse the actions to **reinforce the role of the European Banking Authority in anti-money laundering supervision** of the financial sector and to adopt the relevant legislative measures as soon as possible and by early 2019 at the latest.

Joint Declaration priorities:

- to adopt as a matter of urgency their negotiating mandate on the legislative proposals on **electronic evidence** and enter into trilogue discussions without delay;
- to adopt as a matter of urgency their negotiating mandate on the legislative proposal to **facilitate the use of financial data** and enter into trilogue discussions without delay.

Other:

- to adopt their negotiating mandate by the end of 2018 on the legislative proposal to strengthen the **restrictions on the marketing and use of explosives precursors**;
- to adopt their negotiating mandate by November 2018 on the legislative proposal to enhance the **security features of national identity cards and residence documents**.

⁵⁶ COM(2018) 212 final (17.4.2018).

III. IMPLEMENTATION OF OTHER PRIORITY FILES ON SECURITY

1. Implementation of agreed measures in the Security Union

Action taken by the EU in the Security Union can only provide maximum benefit, and maximum support to national authorities working in the frontline, if Union instruments are fully implemented by all Member States. To achieve this, the Commission is providing support to Member States for full implementation and application of the measures agreed in the Security Union, including by facilitating the exchange of best practices and by providing funding.⁵⁷ But where necessary, the Commission will not hesitate to make full use of all the measures at its disposal for the enforcement of EU law, including infringement action when appropriate, as was done with the following non-communication cases.

With the deadline for the implementation of the **EU Passenger Name Record Directive**⁵⁸ passing on 25 May 2018, the Commission launched infringement procedures on 19 July 2018 against 14 Member States for failing to communicate the adoption of national legislation which fully transposes the Directive⁵⁹ – a vital tool in the fight against terrorism and serious crime. 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 2018 work programme of the Internal Security Fund⁶⁰ foresees further funding of EUR 1.5 million for the interconnectivity of national Passenger Information Units.

The deadline for transposing the **Data Protection Law Enforcement Directive**⁶¹ into national law expired on 6 May 2018. The Commission therefore launched infringement procedures on 19 July 2018 against 19 Member States for failing to communicate the adoption of national legislation which fully transposes the Directive.⁶²

⁵⁷ For example, the Commission has supported Member States throughout the transposition process for the Directive on security of network and information systems (NIS Directive) (see below) on the basis of the September 2017 Communication on Making the most of NIS (COM(2017) 476 final (13.9.2017)). The Commission also published in November 2016 an implementation plan for the EU Passenger Name Record Directive (see below) to support Member States in this process (SWD(2016) 426 final (28.11.2016)).

⁵⁸ Directive (EU) 2016/681 (27.4.2016).

⁵⁹ Austria, Bulgaria, Czech Republic, Estonia, Greece, Spain, France, Cyprus, Luxembourg, Netherlands, Portugal, Romania, Slovenia and Finland. The Commission is receiving replies by Member States, including notifications of the legislation concerned, which are currently being analysed (see also footnote 69).

⁶⁰ C(2018) 6336 (4.10.2018).

⁶¹ Directive (EU) 2016/680 (27.4.2016).

⁶² Belgium, Bulgaria, Czech Republic, Estonia, France, Greece, Spain, Croatia, Cyprus, Latvia, Lithuania, Luxembourg, Hungary, Netherlands, Poland, Portugal, Romania, Slovenia and Finland. The Commission is receiving replies by Member States, including notifications of the legislation concerned, which are currently being analysed (see also footnote 70).

The deadline for transposing the **Directive on security of network and information systems (NIS Directive)**⁶³ into national law expired on 9 May 2018. The Commission therefore launched infringement procedures on 19 July 2018 against 17 Member States for failing to communicate the adoption of national legislation which fully transposes the Directive.⁶⁴ The deadline for the identification of operators that will be subject to the requirements of the Directive, the so-called Operators of Essential Services (OES), will be on 9 November 2018. As part of the sector specific approach to cybersecurity, the Commission is working on guidance to address the requirements of the energy sector with respect to cybersecurity. A high-level conference, jointly organised by the Austrian Presidency and the Commission, will take place on 11 October 2018 in Brussels.

The deadline for transposition of the **Directive on combating terrorism**⁶⁵ expired on 8 September 2018, while the deadline for transposition of the **Directive on the control of the acquisition and possession of weapons**⁶⁶ expired on 14 September 2018. The Commission is currently assessing the notifications received by Member States and will use its powers as guardian of the Treaties to initiate infringement action if and when necessary to ensure full implementation of these instruments. The Commission is also assessing the transposition of the **4th Anti-Money Laundering Directive**⁶⁷ and is working to ensure that the rules are implemented on the ground. The Commission has launched infringement procedures against 20 Member States for failing to communicate the adoption of national legislation transposing the Directive.⁶⁸ It will continue to use its powers when appropriate to ensure full implementation of this Directive.

The Commission calls on all Member States to fully implement and apply all EU measures and instruments agreed in the Security Union.

⁶³ Directive (EU) 2016/1148 (27.4.2016).

⁶⁴ Austria, Bulgaria, Belgium, Croatia, Denmark, France, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Netherlands, Poland, Portugal, Romania and Spain. The Commission is receiving replies by Member States, including notifications of the legislation concerned, which are currently being analysed (see also footnote 71).

⁶⁵ Directive (EU) 2017/541 (15.3.2017).

⁶⁶ Directive (EU) 2017/853 (17.5.2017).

⁶⁷ Directive (EU) 2015/849 (20.5.2015).

⁶⁸ Austria, Belgium, Bulgaria, Cyprus, Estonia, Greece, Spain, France, Finland, Croatia, Ireland, Lithuania, Latvia, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania and Slovakia.

Since the transposition deadline has expired, 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 this to the Commission:

- the **EU Passenger Name Record Directive**, where 8 Member States still need to notify transposition into national law and 2 Member States need to complete the notification of transposition;⁶⁹
- the **Data Protection Law Enforcement Directive**, where 11 Member States still need to notify transposition into national law and 2 Member States need to complete the notification of transposition;⁷⁰
- the **Directive on security of network information systems**, where 8 Member States still need to notify transposition into national law and 3 Member States need to complete the notification of transposition;⁷¹
- the **Directive on combating terrorism**, where 9 Member States still need to notify transposition into national law and 10 Member States need to complete the notification of transposition;⁷²
- the **Directive on the control of the acquisition and possession of weapons**, where 21 Member States still need to notify transposition into national law and 5 need to complete the notification of transposition;⁷³ and
- the **4th Anti-Money Laundering Directive**, where 1 Member State still needs to notify transposition into national law and 3 Member States need to complete the notification of transposition.⁷⁴

⁶⁹ Cyprus, Greece, Spain, Finland, Netherlands, Portugal, Romania and Slovenia are yet to communicate transposition. The Czech Republic and Estonia communicated partial transposition and are yet to complete the notification of transposition.

⁷⁰ Bulgaria, Cyprus, Estonia, Greece, Finland, Spain, Latvia, Netherlands, Poland, Romania and Slovenia are yet to communicate transposition. The Czech Republic and Portugal communicated partial transposition and are yet to complete the notification of transposition.

⁷¹ Austria, Bulgaria, Belgium, Greece, Latvia, Luxembourg, Netherlands and Romania are yet to communicate transposition. Poland, Lithuania and Hungary communicated partial transposition and are yet to complete the notification of transposition.

⁷² Bulgaria, Germany, Greece, Italy, Cyprus, Luxembourg, Malta, Romania and Finland are yet to communicate transposition. Austria, Belgium, Croatia, Czech Republic, Estonia, France, Lithuania, Portugal, Slovenia and Spain communicated partial transposition and are yet to complete the notification of transposition.

⁷³ Belgium, Bulgaria, Germany, Estonia, Ireland, Greece, Spain, Croatia, Cyprus, Latvia, Luxembourg, Hungary, Malta, Netherlands, Austria, Poland, Romania, Slovenia, Slovakia, Finland and Sweden are yet to communicate transposition. The Czech Republic, France, Portugal, Lithuania and the United Kingdom communicated partial transposition and are yet to complete the notification of transposition.

⁷⁴ Romania is yet to communicate transposition. Austria, Ireland and Luxembourg communicated partial transposition and are yet to complete the notification of transposition. The remaining 16 Member States have notified full transposition and the assessment by the Commission is ongoing.

2. Protection of public spaces

To improve our protection and resilience against terrorism, the Commission is continuing to support Member States in **protecting public spaces**, implementing the October 2017 Action Plan⁷⁵ with measures to support action at national, regional and local level. The Operators Forum, a Commission-led group to encourage public-private security partnerships and engage with private operators, held a thematic meeting with the hospitality and commerce sector on 26-27 September 2018, bringing together stakeholders from restaurants, hotels, hospitals, shopping malls and convention centres. The full meeting of the Operators Forum involving all sectors will take place on 26-27 November 2018. To foster the exchange of best practices, the Commission is proposing to select projects for EUR 25.4 million in funding as result of a 2017 call for proposals through the Internal Security Fund. In addition, during the European Week of Regions and Cities on 8-11 October 2018 the Commission will launch a call under Urban Innovative Actions as part of the European Regional Development Fund.⁷⁶ Security will be one of the four topics under this call, which has total funding of EUR 100 million and a deadline for applications in January 2019. Moreover, under the framework of the Urban Agenda for the EU, the Commission has proposed a partnership on security in public spaces⁷⁷ that will allow Member States, cities representatives and other stakeholders to develop jointly an action plan for better regulation, knowledge and funding to enhance security in public spaces.

As part of the 2018 work programme of the Internal Security Fund⁷⁸, the Commission launched together with this report a call for proposals for further funding of EUR 9.5 million for the protection of public spaces as well as funding for proposals addressing chemical, biological, radiological and nuclear (CBRN) threats, supporting critical infrastructure protection and restricting access to explosives and explosives precursors. In addition, the Commission is continuing its work on implementing the Joint Communication⁷⁹ on Increasing resilience and bolstering capabilities to address hybrid threats as well as the Action Plan⁸⁰ to enhance preparedness against chemical, biological, radiological and nuclear security risks in response to the call by the March 2018 European Council to strengthen resilience to these risks.

3. External dimension

The EU and Canada launched formal negotiations on 20 June 2018 on a **revised Passenger Name Record Agreement between the EU and Canada**. A second negotiation round took place in Ottawa on 18-19 September 2018 which is currently being followed up at a technical level. The Commission debriefed the Council at working group level on 1 October 2018 and will debrief the European Parliament's LIBE Committee in the coming days on the good progress made in the negotiations.

⁷⁵ COM(2017) 612 final (18.10.2017).

⁷⁶ <http://www.uia-initiative.eu/en>.

⁷⁷ <https://webgate.ec.europa.eu/playground-multisite/futurium/en/urban-agenda/terms/all/Security%20in%20public%20spaces>.

⁷⁸ C(2018) 6336 final (4.10.2018).

⁷⁹ JOIN(2018) 16 final (12.6.2018). This includes additional measures set out in the Fifteenth Progress Report towards an effective and genuine Security Union (COM(2018) 470 final (13.6.2018)).

⁸⁰ COM(2017) 610 final (18.10.2017).

As part of enhanced EU engagement with the Western Balkans on security⁸¹, the Commission, on behalf of the EU, signed together with all six Western Balkans partners a **Joint Action Plan on Counter-Terrorism for the Western Balkans** at the EU-Western Balkans Justice and Home Affairs Ministerial Meeting in Tirana on 5 October 2018.⁸² The Action Plan will provide a common focus and a jointly agreed basis for concrete deliverables in order to tackle the existing security challenges, including a systematic strengthening of regional cooperation. Its five objectives include setting up a robust framework for countering terrorism, ensuring effective prevention and countering of violent extremism, ensuring effective information exchange and operational cooperation, building capacity to combat money laundering and terrorism financing, and strengthening the protection of citizens and infrastructure. For each objective, it indicates actions for the Western Balkans partners (including a regional dimension) as well as actions for EU support. Moreover, under the Digital Agenda for the Western Balkans, the EU is seeking to step up its cooperation with the Western Balkans partners on cybersecurity, in particular with the support of the EU Agency for Network and Information Security (ENISA).

Following the initialling of status agreements on operational cooperation with Albania in February 2018 and with the former Yugoslav Republic of Macedonia in July 2018, the Commission and the Republic of Serbia initialled on 20 September 2018 a **status agreement on operational cooperation with Serbia** that will allow European Border and Coast Guard teams to be deployed in the country. On 5 October, the status agreement with Albania was signed. The Agency will be able to assist these Western Balkan partners in border management and carry out joint operations, in particular in the event of a sudden change in migratory flows. Negotiations are ongoing with Montenegro and Bosnia and Herzegovina.

The EU participated in the first **high-level conference of heads of counter-terrorism agencies** organised by the UN Secretary General, together with the UN Office of Counter Terrorism, on 28-29 June 2018. Over 1,000 participants from 150 countries, 51 civil society organisations as well as 30 international and regional organisations convened to strengthen multilateral counter-terrorism cooperation and build new partnerships to address the complex and transnational threat from terrorism.

The **EU-US Senior Officials Meeting on Justice and Home Affairs** on 25-26 September 2018 in Vienna addressed security-related aspects of transatlantic cooperation such as law enforcement cooperation and the exchange of passenger name record data, aviation security and cooperation on chemical threats, preparing the EU-US Ministerial Meeting on Justice and Home Affairs that will take place in Washington on 8-9 November 2018.

The **EU-Australia Counter-Terrorism Dialogue** on 12 July 2018 in Brussels addressed cooperation with Europol, the exchange of passenger name record data, Australian efforts to counter terrorism and violent extremism in South East Asia and cooperation in the Global Counter Terrorism Forum and the Anti-Isil Coalition.

As part of EU efforts to strengthen cooperation in the area of security and counter-terrorism with Southern partners, a **joint senior EU mission visited Algeria** on 16-18 July 2018. Discussions focused on counter-terrorism efforts in the Sahel.

⁸¹ Security and migration are one of the thematic flagship initiatives under the February 2018 Communication on A credible enlargement perspective for and enhanced EU engagement with the Western Balkans (COM(2018) 65 final (6.2.2018)).

⁸² Council Document 12411/18.

IV. CONCLUSION

Europeans expect their Union to keep them safe, as President Juncker underlined in his 2018 State of the Union address. The coming months will be decisive to deliver on all pending legislative proposals in the Security Union ahead the European Parliament elections in May 2019, in line with the Joint Declaration on the EU's legislative priorities for 2018-19 and the positive momentum from the informal Leaders' Meeting in Salzburg.

Building on the progress made towards an effective and genuine Security Union over the last few years, the Commission calls on the European Parliament and the Council to continue to work as a matter of urgency on the priority legislative initiatives agreed in the Joint Declaration and the latest Security Union initiatives put forward by the Commission with the 2018 State of the Union. Where necessary, the co-legislators need to accelerate this work to reach agreement on all files during the current term of the European Parliament.