Council of the European Union

Brussels, 25 March 2019
(OR. en)

7434/19

JAI 331
COSI 57
FRONT 120
ASIM 38
DAPIX 117
ENFOPOL 122
SIRIS 57
VISA 70
FAUXDOC 26
COPEN 128
CYBER 105
DATAPROTECT 108
CT 29
JAIEX 49
EF 124

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	21 March 2019
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2019) 145 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Eighteenth Progress Report towards an effective and genuine Security Union

Delegations will find attached document COM(2019) 145 final.

Encl.: COM(2019) 145 final

EUROPEAN
COMMISSION

Brussels, 20.3.2019
COM(2019) 145 final

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

Eighteenth Progress Report towards an effective and genuine Security Union

{SWD(2019) 140 final}

I. INTRODUCTION

This is the eighteenth report on the further progress made towards building an effective and genuine Security Union. It 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.

Ahead of the European Parliament elections in May 2019, this report underlines the important work undertaken at various levels to address and prevent cyber threats and disinformation in the electoral context. In response to the European Council's call for measures to protect the Union's democratic systems and to combat disinformation in the run-up to the upcoming elections, the Union has made considerable progress towards more coordinated action on electoral resilience. However, given the time pressure to ensure the Union's preparedness before European voters go the polls in May 2019, the Commission calls on all actors involved – government authorities, political parties and notably online platforms – to redouble their efforts to step up electoral resilience to counter disinformation. Ahead of the upcoming European Council on 21 and 22 March 2019 that will discuss progress in this area, the Commission also calls on Member States to strengthen their coordination to address disinformation and ensure the protection of the European Parliament elections.

The EU has made considerable progress in the work towards an effective and genuine Security Union, with agreement reached on a number of priority legislative initiatives that will enhance security for all citizens. Over recent months[1], the European Parliament and the Council reached agreement on the interoperability of EU information systems for security, border and migration management, and on new EU rules to close down the space in which terrorists and criminals operate, making it harder for them to access explosives precursors, finance their activities and travel without detection. With agreement reached on 15 out of 22 legislative initiatives presented by the Commission in the Security Union (see list of all Security Union initiatives in *Annex I*), the EU is delivering in what is a joint priority area for the European Parliament, the Council and the Commission.[2]

However, there is a need for further efforts. In particular, within the current legislative mandate, the co-legislators need to address the urgent threat posed by terrorist content online, by reaching agreement on the Commission's proposal. The European Parliament and the Council also need to reach agreement on the Commission's proposal for a reinforced European Border and Coast Guard to strengthen security through enhanced protection of the external borders of the Union.

The tragic events in Christchurch, New Zealand on 15 March 2019 show that the threat of terrorism remains a clear and present danger, whether fuelled by far right extremism or other extremist ideologies. The difficulties encountered in trying to remove live-streamed content from Internet platforms and prevent its reappearance further underlines the vital importance of the Commission's proposal on terrorist content online. It is crucial that the proposed rules for the removal of terrorist content online are agreed by the co-legislators as a matter of urgency.

---

1 This builds on earlier progress made in the work towards an effective and genuine Security Union. For a complete overview, see previous Security Union progress reports: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

2 See the Joint Declaration on the EU's legislative priorities for 2018-19: https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-eu-legislative-priorities-2018-19_en.pdf.

It is equally important to the fight against terrorism in all its forms that all Member States fully implement legislation the EU has adopted notably in response to terrorist attacks in Europe to close down the space in which terrorists operate, in particular the Directives on combating terrorism and on the control of acquisition and possession of firearms. In the context of fighting extremism, the Commission has also been actively working, and taking relevant measures, against illegal hate speech online, anti-Muslim hatred and Antisemitism.

This report also sets out the progress made in the implementation of other priority files on security, notably on measures to support the protection of public spaces. The complete and correct implementation of agreed measures is of the utmost priority to ensure the full benefits of an effective and genuine Security Union. The Commission is actively supporting Member States, including through funding and by facilitating the exchange of best practices. Where necessary, the Commission also makes full use of its powers under the Treaties for the enforcement of EU law, including infringement action when appropriate.

The commemoration of the 15th European Remembrance Day for Victims of Terrorism on 11 March 2019, fifteen years after the Madrid Bombings of 11 March 2004 and three years after the deadly attacks in Brussels and Zaventem of 22 March 2016, is the backdrop of this report. Providing support to victims of terrorist attacks is an important part of the work towards an effective and genuine Security Union. To further step up this support, the Commission adopted on 31 January 2019 a Decision on the financing of the pilot project "Setting up a EU Centre of Expertise for Victims of Terrorism".[3] The EU Centre of Expertise will act as a hub of expertise and platform for practitioners dealing with victims of terrorism.

The Commission welcomes the contribution of the European Parliament's Report on findings and recommendations of the Special Committee on Terrorism[4] as a valuable input to the joint work towards an effective and genuine Security Union.

II. DELIVERING ON LEGISLATIVE PRIORITIES

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

Information exchange is a central aspect of the support the EU provides to national authorities in the fight against terrorism and serious crime. In that respect, the interoperability of EU-wide information systems marks a step change in the way data is provided to national authorities, ensuring that data is accurate and complete. The co-legislators have reached political agreement on the related priority legislative proposals to achieve the **interoperability of EU information systems** for security, border and migration management.[5] The proposed measures will make EU information systems work together in a more intelligent and targeted way whilst fully respecting fundamental rights. Making best use of existing data, interoperability will close information gaps and blind spots by helping to detect multiple identities and countering identity fraud. Once the co-legislators formally adopt the new rules, the Commission will stand ready to support Member States in their

---

3 C (2019)636 (31.1.2019).

4 European Parliament resolution of 12 December 2018 on findings and recommendations of the Special Committee on Terrorism (2018/2044(INI)).

5 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). The political agreement reached on 5 February 2019 was endorsed by the Council's Committee of the Permanent Representatives on 13 February 2019 and by the European Parliament's Civil Liberties, Justice and Home Affairs Committee on 19 February 2019.

implementation. There is a need for close cooperation with EU agencies and all Member States and Schengen associated countries to reach the ambitious objective of achieving full interoperability of EU information systems for security, border and migration management by 2020. In preparation of that, a first workshop took place with Member States' experts on 5 March 2019 to launch a process of effective coordination.

At this stage, the future architecture of interoperable EU information systems will include the reinforced **Schengen Information System**[6], the existing **Visa Information System**[7], the recently agreed extension of the **European Criminal Records Information System**[8] to third-country nationals, and the newly established **EU Entry/Exit System**[9] and **European Travel Information and Authorisation System (ETIAS)**[10].

As part of the technical implementation of the European Travel Information and Authorisation System, the Commission put forward a proposal on 7 January 2019 setting out technical amendments to the related Regulation.[11] The proposed changes concern the legal acts of those EU information systems that the European Travel Information and Authorisation System will query as part of the assessment of security or irregular migration risks of visa-exempt third-country nationals prior to their travel to the Schengen Area. The proposed amendments are necessary to fully set up the European Travel Information and Authorisation System. The Commission calls on the co-legislators to advance their work on the 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**[12] 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 next European Parliament.

In May 2016, the Commission proposed to extend the scope of **Eurodac**[13] 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[14] and the Commission Communication of 6 March 2019 on progress in

6 Regulation (EU) 2018/1860 (28.11.2018), Regulation (EU) 2018/1861 (28.11.2018), Regulation (EU) 2018/1862 (28.11.2018).
7 Regulation (EC) 767/2008 (9.7.2008).
8 The co-legislators reached political agreement on this priority proposal on 11 December 2018 (COM(2017) 344 final (29.6.2017)). The Council's Committee of the Permanent Representatives endorsed the agreement on 19 December 2018. The European Parliament's Plenary confirmed the agreement on 11 March 2019.
9 Regulation (EU) 2017/2226 (30.11.2017).
10 Regulation (EU) 2018/1240 (12.9.2018) and Regulation (EU) 2018/1241 (12.9.2018).
11 COM(2019) 4 final (7.1.2019).
12 COM(2018) 302 final (16.5.2018).
13 COM(2016) 272 final (4.5.2016).
14 https://www.consilium.europa.eu/en/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/.

the implementation of the European Agenda on Migration,[15] the Commission calls on the co-legislators to proceed to the adoption of the proposal without delay. Adopting this legislative proposal will 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,** on which agreement is within close reach, before the European Parliamentary elections. (*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.**

2. Strengthening security through enhanced external border management

Strong protection of the external borders is a precondition for security in the area of free movement without internal border controls. This is a task for the Member States, who have to ensure the management of their external borders both in their own interests and in the common interest of all, with the help of the **European Border and Coast Guard**. In response to the European Council conclusions of June 2018[16], the Commission proposed in September 2018 to enhance the capacities of the European Border and Coast Guard.[17] It would take the Agency to a new operational level with a standing corps of 10 000 border guards exercising executive powers and with its own equipment, while fully respecting both fundamental rights and the sovereignty of the Member States.

The legislative work on the proposal is advancing well and negotiations between the co-legislators have entered into the crucial phase. The European Parliament adopted its negotiating mandate on 11 February 2019, while the Council received its mandate on 20 February 2019. Two trilogue meetings took place on 27 February 2019 and 12 March 2019. The Commission welcomes and supports the progress made on this priority file, showing that all institutions are committed towards adopting this proposal before the 2019 European Parliament elections.

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

- to adopt the legislative proposal to strengthen the **European Border and Coast Guard** during the current term of the European Parliament. (*2018 State of the Union initiative*)

3. Preventing radicalisation

Addressing terrorist content online remains a key challenge in fighting terrorism and preventing radicalisation. Such content has had a role to play in most attacks on European soil in the last two years, whether through incitement to commit an attack, instructions on how to carry it out or glorification of the deadly results. In order to tackle the clear and present

15 COM(2019) 126 final (6.3.2019).
16 https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf.
17 COM(2018) 631 final (12.9.2018).

danger posed by such content, President Juncker's 2018 State of the Union address was accompanied by a proposal[18] for a Regulation on **terrorist content online**, setting out a legal framework to prevent the misuse of hosting service providers for the dissemination of terrorist content online. While fully guaranteeing freedom of speech and other fundamental rights, it is critical for the future rules to provide for effective measures to remove terrorist content online as rapidly as possible, given that the potential damage caused by such content rises with every hour it remains online.

While the Council adopted its negotiating mandate in December 2018, work in the European Parliament is still ongoing and will hopefully allow the Parliament to adopt its negotiating mandate in the course of March 2019.[19] The Commission calls on both co-legislators to reach agreement on the proposed legislation during the current term of the European Parliament, given the vital importance of an EU regulatory framework for the removal of terrorist content online with clear rules and safeguards.

In parallel, the Commission continues to provide support to Member States in their efforts to **prevent radicalisation**. A dedicated EU Cooperation Mechanism, bringing together national representatives, helps ensure that EU-level support responds to Member States' needs.[20] Recent examples include a conference on "EU cities against radicalisation" jointly organised with the Committee of the Regions on 26 February 2019. On 13 March 2019, the Commission organised an expert meeting with national policymakers to identify practical steps to further support prison and probation services. The outcome of this work will become part of a manual which the Radicalisation Awareness Network is preparing on the rehabilitation and reintegration of terrorist offenders, returning foreign terrorist fighters and those radicalised in prison (see also section IV.4 on external).

In order to prevent radicalisation, the Commission calls on the European Parliament:
• to adopt, as a matter of priority, its negotiating mandate on the legislative proposal to prevent the dissemination of **terrorist content online**, in order for the co-legislators to reach agreement on the legislation during the current term of the European Parliament. (*2018 State of the Union initiative*)

4. Enhancing cybersecurity

Classic cyber threats to systems and data remain on the rise, with an increase in activity from malicious actors across a diverse range of targets and victims in 2018. Countering cybercrime and enhancing cybersecurity therefore remains a priority for EU action. The EU has made tangible progress in enhancing its cybersecurity, implementing the actions set out in the

18 COM(2018) 640 final (12.9.2018).

19 The European Parliament's Committee on Internal Market and Consumer Protection voted on its opinion on 4 March 2019. The European Parliament's Committee on Culture and Education voted on its report on 11 March 2019. The European Parliament's Civil Liberties, Justice and Home Affairs Committee is expected to vote on its report on 21 March 2019.

20 Member States' needs in the prevention of radicalisation have been identified, for the first time, in the so-called strategic orientations for EU prevent actions for 2019. The strategic orientations are accessible under: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3626&news=1&mod_groups=1&month=08&year=2018.

September 2017 Joint Communication[21] on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU".

On 12 March 2019, the European Parliament's Plenary confirmed the political agreement reached by the co-legislators on the **Cybersecurity Act**. With entry into force expected in May 2019, the Act will increase cybersecurity capabilities and the preparedness of Member States and businesses. The Cybersecurity Act will establish an EU cybersecurity certification framework for information and communications technology products, systems and services. It will also improve cooperation and coordination across Member States and EU institutions, agencies and bodies, notably the renamed EU Agency for Cybersecurity.

Further progress is needed, however, on the September 2018 Commission proposal on a **European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres**.[22] The proposal aims to support cybersecurity technological and industrial capacities and to increase the competitiveness of the Union's cybersecurity industry. The European Parliament and the Council adopted their negotiating mandates on 13 March 2019. The first trilogue meeting also took place on 13 March 2019. The Commission calls on the co-legislators to reach swift agreement on the proposed legislation.

The EU has made significant progress towards further operationalisation of the **Joint EU Diplomatic Response to Malicious Cyber Activities** (the "cyber diplomacy toolbox"), responding to the call by the European Council[23] to take forward the work on the capacity to respond to and deter cyber-attacks through EU restrictive measures. On 8 March 2019, the High Representative of the Union for Foreign Affairs and Security Policy and the Commission presented a joint proposal for a Council Regulation concerning restrictive measures to counter cyber-attacks threatening the Union or its Member States. The Commission and the High Representative call for the swift adoption of this proposal to strengthen the Union's resilience against cyber-attacks.

In order to enhance cybersecurity, the Commission and the High Representative call on the Council:
• to adopt the Council Regulation concerning **restrictive measures to counter cyber-attacks** threatening the Union or its Member States.

5. Closing down the space in which terrorists operate

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

The European Parliament and the Council reached political agreement on 14 February 2019 on the proposed Regulation on **restrictions on the marketing and use of explosives precursors**.[24] Once applicable, the Regulation will make significant improvements to the current legislative framework, restricting access to dangerous explosives precursors that might

21 JOIN(2017) 450 final (13.9.2017).
22 COM(2018) 630 final (12.9.2018).
23 See the June 2018 and October 2018 European Council Conclusions.
24 COM(2018) 209 final (17.4.2018).

be misused to build homemade bombs. It will close security gaps with measures such as banning additional chemicals, 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.

Moreover, as part of the efforts to fight terrorist financing, the co-legislators reached agreement on the proposed Directive to **facilitate the use of financial and other information** for the prevention, detection, investigation or prosecution of serious criminal offences.[25] Once formally adopted and implemented, the Directive will provide designated law enforcement authorities and Asset Recovery Offices with direct access to bank account information held in national centralised bank account registries. The Directive will also enhance the cooperation between national Financial Intelligence Units and law enforcement authorities and facilitate Europol's access to financial information.

Building on that, the Commission will further reflect on cooperation between Financial Intelligence Units of different Member States, including in the upcoming report on the cooperation between Financial Intelligence Units as foreseen by the 5th Anti-Money Laundering Directive.[26] In addition, as also required by the 5th Anti-Money Laundering Directive, the Commission is assessing aspects related to the potential interconnection of national centralised bank account registries and data retrieval systems in the EU. The Commission is also analysing non-conviction based confiscation measures in the Union. Finally, and also in response to a call by the European Parliament,[27] the Commission will continue to assess the necessity, technical feasibility and proportionality of additional measures to track terrorist financing in the EU.

As part of the work to curb document fraud, the co-legislators reached provisional agreement on 19 February 2019 on the proposed Regulation to strengthen the **security of identity cards of Union citizens and of residence documents**[28] so that they cannot be used fraudulently by criminals and terrorists. The European Parliament's Civil Liberties, Justice and Home Affairs Committee confirmed the agreement on 11 March 2019. Once adopted, the Regulation will introduce minimum security features for identity cards including biometric identifiers (a facial image and two fingerprints) on a contactless chip. This will significantly improve the security of national identity cards and residence documents, making it more difficult for terrorists and other criminals to misuse or falsify such documents to enter or move within the EU. More secure identity documents will contribute to strengthening EU external border management. At the same time, more secure and reliable documents will make it easier for EU citizens to exercise their free movement rights.

---

25 The co-legislators reached political agreement on the Commission proposal on 12 February 2019 (COM(2018) 213 final (17.4.2018)). This was endorsed by the Council's Committee of the Permanent Representatives on 20 February 2019 and by the European Parliament's Civil Liberties, Justice and Home Affairs Committee on 26 February 2019.

26 Article 65(2) of Directive (EU) 2018/843 (19.6.2018) sets out that by 1 June 2019, the Commission shall assess the framework for Financial Intelligence Units' cooperation with third countries and obstacles and opportunities to enhance cooperation between Financial Intelligence Units in the Union including the possibility of establishing a coordination and support mechanism.

27 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.

28 COM(2018) 212 final (17.4.2018).

Further progress is needed, however, on the Commission's April 2018 proposals on **access to electronic evidence**, given that more than half of all criminal investigations today involve a cross-border request to access electronic evidence.[29] The Council adopted its negotiating mandate on proposals for a Regulation[30] to improve the cross-border access to electronic evidence in criminal investigations and for a Directive[31] laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. In the European Parliament, however, there has only been very limited progress on the proposals since their adoption by the Commission in April 2018. Given the crucial importance of efficient access to electronic evidence for the prosecution of cross-border crimes such as terrorism or cybercrime, the Commission urges the European Parliament to advance on this proposal.

In parallel, the Commission is working on its **international initiatives on access to electronic evidence** in the context of ongoing negotiations of a Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime and with the United States. Therefore, the Commission adopted recommendations[32] for negotiation mandates for both of these international initiatives on 5 February 2019. The Council is currently discussing the draft mandates, including at the 7-8 March 2019 Justice and Home Affairs Council meeting. The Commission calls on the Council to adopt the Decision authorising the participation in negotiations on a Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime, as well as the Decision authorising the opening of negotiations with the United States on cross-border access to electronic evidence. It is important to proceed fast with the negotiations in order to advance international cooperation on sharing electronic evidence, while ensuring compatibility with EU law and Member States' obligations under it, taking also account of future developments in EU law.

In order to close down the space in which terrorists operate, the Commission calls on:

- the **European Parliament** to adopt as a matter of urgency its negotiating mandate on the legislative proposals on **electronic evidence** in order to enter into trilogue discussions with the Council without delay. (*Joint Declaration priority*)
- the **Council** to adopt the Decisions authorising the participation in negotiations on a **Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime** as well as the opening of **negotiations with the United States** on cross-border access to electronic evidence.

III. COUNTERING DISINFORMATION AND PROTECTING ELECTIONS AGAINST OTHER CYBER-ENABLED THREATS

The ability of outside and inside parties to interfere in public debates and manipulate elections is more real than ever and could increase further with the upcoming European Parliament elections. The possible consequences – the undermining or delegitimising of democratic

[29] 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)).

[30] 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.

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

[32] COM(2019) 70 final (5.2.2019) and COM(2019) 71 final (5.2.2019).

institutions – are a serious, strategic and growing threat. They are a key part of the security challenges the EU faces today across national borders, and require a joint, cross-border response.

The electoral campaigns ahead of the European Parliament elections will start in earnest in March. Ahead of the European Council on 21 and 22 March 2019, the Commission calls on Member States to step up their coordination and information exchange to counter disinformation and protect elections against cyber-enabled threats. Member States should make full use of the tools and information channels provided by the EU, notably the newly established Rapid Alert System.[33] Moreover, due to concern for the situation as it stands, the Commission urges online platforms to accelerate their efforts across all Member States to help ensure the integrity of the European Parliament elections in May 2019.

To support and encourage these efforts, the Commission and the High Representative continue to take action along two complementary strands to address cyber-enabled threats: countering disinformation and enhancing electoral resilience.

1. Taking Action against Disinformation

The exposure of citizens to large-scale disinformation, including misleading or outright false information, may be a serious type of cyber-enabled threat and is a major challenge for the upcoming European elections. The Commission is closely monitoring the implementation of the actions set out in its **April 2018 Communication on Tackling online disinformation**.[34]

Moreover, progress made under the **Code of Practice on Disinformation**, signed by representatives of online platforms, leading social networks, advertisers and the advertising industry in October 2018, is under close monitoring by the Commission (see below). The Commission will carry out a comprehensive assessment at the conclusion of the Code's initial 12-month period of application. Should the implementation and the impact of the Code of Practice prove to be unsatisfactory, the Commission may propose further measures, including of a legislative nature.

Building on this work, and responding to the call made by Leaders at the June 2018 European Council to protect the Union's democratic systems, the Commission and the High Representative presented a **Joint Action Plan against disinformation**[35] in December 2018. The Action Plan highlights that, according to the **EU Hybrid Fusion Cell,** disinformation by the Russian Federation poses the greatest threat to the EU. It is systematic, well-resourced and on a different scale compared to other countries. To address the threat posed by disinformation, the Action Plan foresees an increase of resources devoted to the fight against disinformation, more specifically for the **Strategic Communication Task Forces** of the European External Action Service (EEAS), including the East Strategic Communication Task

---

33 As part of the Action Plan against disinformation presented by the Commission and the High Representative in December 2018 (see below), the Rapid Alert System will be a hub for Member States, EU institutions and partners to share information on ongoing disinformation campaigns and allow them to coordinate their responses. The system will be based on open-source and unclassified information only.

34 COM(2018) 236 final (26.4.2018), followed up with an implementation report (COM(2018) 794 final (5.12.2018)).

35 JOIN(2018) 36 final (5.12.2018).

Force.[36] The Action Plan also foresees an increase of resources devoted to the issue, and calls for a reinforcement over the next two years.

The Action Plan set out concrete measures to tackle disinformation, including the creation of a **Rapid Alert System**. With a view to the European Parliament elections, the Rapid Alert System was set up in March 2019 among the EU institutions and Member States to facilitate the sharing of data and assessments of disinformation campaigns and to provide alerts on disinformation threats.

The Action Plan also foresees close monitoring of the implementation of the above-mentioned Code of Practice signed by the online platforms. On 29 January 2019, the Commission published the **reports submitted by signatories of the Code of Practice** – Google, Facebook, Twitter, Mozilla and the trade associations representing the advertising sector. While the Commission welcomed progress made, it also called on signatories to intensify their efforts in the run up to the 2019 European Parliament elections.[37]

On 28 February 2019, the Commission published **reports by Facebook, Google and Twitter** covering the progress made in January 2019 on their commitments to fight disinformation. In these reports, platforms did not provide enough details showing that new policies and tools are being deployed in a timely manner and with sufficient resources across all Member States. There is clearly room for improvement for all signatories.[38] More specifically, the Commission calls for platforms to ensure transparency of political ads by the start of the campaign for the European elections in all EU Member States, to allow appropriate access to platforms' data for research and fact-checking purposes, and to ensure proper cooperation between the platforms and individual Member States through contact points in the Rapid Alert System.

The Commission will report again on 20 March 2019 on the implementation of the above-mentioned Code of Practice.

2. Enhancing Electoral Resilience

On 12 September 2018 the Commission adopted a package of measures to enhance the resilience of our electoral systems addressed to Member States and European and national political parties and foundations, including a Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns, guidance on the application of EU data protection law,[39] and a legislative amendment to tighten the rules on European political party funding.

The European Parliament welcomed the package in its Resolution adopted on 28 October 2018. The Council welcomed the package in its Conclusions of 19 February 2019 on securing free and fair European elections, which express a shared commitment by all Member States to

---

36 Since its establishment in 2015, the East Strategic Communication Task Force has catalogued, analysed and put the spotlight on almost 5,000 examples of disinformation by the Russian Federation, uncovering numerous disinformation narratives, raising awareness of and exposing the tools, techniques and intentions of disinformation campaigns.

37 For further details, see: http://europa.eu/rapid/press-release_IP-19-746_en.htm.

38 For further detail, see: http://europa.eu/rapid/press-release_STATEMENT-19-1379_en.htm.

39 COM(2018) 638 final (12.9.2018).

a coordinated European approach to protecting the integrity of the upcoming European elections. The Justice and Home Affairs Council discussed the state of play on 7 March 2019.

The amendment to the Regulation on the **statute and funding of the European political parties and foundations**[40] introduces the possibility to impose sanctions on the illegal use of personal data in case of deliberate impact on the outcome of the European Parliament elections. Following political agreement[41] in January 2019, the European Parliament's Plenary approved the text of the amendment on 12 March 2019. The amendment is scheduled to become law ahead of 2019 European Parliament elections.

The Recommendation on **election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament**[42] is addressed to the Member States and national and European political parties and foundations and presents concrete steps for relevant actors in these areas. In an effort to implement the Recommendation, national election networks appointed contact points to take part in a **European cooperation network on elections** that serves to raise alerts about threats, exchange on best practices among national networks, discuss common solutions to identified challenges and encourage common projects and exercises among national networks. At the first meeting of the network on 21 January 2019, participants agreed that a comprehensive approach is essential to ensure the integrity of elections while preserving an open democratic debate and a level political playing field. The second meeting of the European cooperation network on elections took place on 27 February 2019, focussing on monitoring and enforcement related topics relevant to the electoral context, including data protection, media regulation, law enforcement, transparency and social media, and engagement of different stakeholders in monitoring activities. It laid the groundwork for its membership to participate in a cyber-resilience exercise immediately after the network's next anticipated meeting on 5 April 2019.

A **Workshop on "Enhancing cyber resilience of elections"**, jointly organised by the European Parliament and the Commission, was held on 19 February 2019 to improve the security and resilience of electoral systems and infrastructures against constantly evolving cyber-enabled threats. National cybersecurity authorities from Member States, the European Union Agency for Network and Information Security and online platforms discussed measures focusing on actions that are urgent and relevant for ensuring the integrity of the 2019 European Parliament elections.

The EU institutions and the Member States are also closely cooperating on other **awareness-raising activities** aimed at protecting the integrity of the electoral process and on involving actors from the private and public sector, including media, online platforms and civil society.

In order to address disinformation and ensure electoral resilience, the Commission and the High Representative call on the Member States:

- to implement swiftly and decisively the actions of the December 2018 **Joint Action Plan against Disinformation**.

40 COM(2018) 636 final (12.9.2018).

41 The co-legislators reached political agreement on 16 January 2018, which was endorsed by the Council's Committee of the Permanent Representatives on 25 January 2019 and by the European Parliament's Committee on Constitutional Affairs on 29 January 2019.

42 C(2018) 5949 final (12.9.2018).

IV. IMPLEMENTATION OF OTHER PRIORITY FILES ON SECURITY

1. Implementation of legislative measures in the Security Union

The complete and correct implementation of agreed measures is of utmost priority to ensure the full benefits of an effective and genuine Security Union. The Commission is actively supporting Member States, including through funding and by facilitating the exchange of best practices. Where necessary, the Commission also makes full use of its powers under the Treaties for the enforcement of EU law, including infringement action when appropriate.

As regard the implementation of the **EU Passenger Name Record Directive**[43], 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 Directive[44] – a critical tool in the fight against terrorism and serious crime. Nine of those Member States have since notified full transposition[45]. Member States where full transposition is still absent have received reasoned opinions (Spain on 24 January 2019, the Netherlands and Finland on 7 March 2019). 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**[46] expired on 8 September 2018. The Commission launched infringement procedures on 22 November 2018 against 16 Member States for failing to communicate the adoption of national legislation which fully transposes the Directive. 9 of these Member States have since notified full transposition[47]. The Commission urges the remaining 7 Member States to take the necessary measures as soon as possible[48].

The deadline for transposition of the **Directive on the control of the acquisition and possession of weapons**[49] expired on 14 September 2018. So far, 6 Member States have notified full transposition[50] and 5 Member States have notified partial transposition[51]. 22 Member States[52], including those that have notified partial transposition, received the Commission's letters of formal notice on 22 November 2018.

---

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

44 Bulgaria, Czechia, Estonia, Greece, Spain, France, Cyprus, Luxembourg, the Netherlands, Austria, Portugal, Romania, Slovenia and Finland.

45 Bulgaria, Estonia, Greece, France, Cyprus, Luxembourg, Austria, Portugal, Romania (state of play as of 11 March 2019).

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

47 Bulgaria, Czechia, Germany, Estonia, Spain, France, Croatia, Italy, Latvia, Lithuania, Hungary, Malta, the Netherlands, Austria, Portugal, Slovakia, Finland and Sweden notified transposition (state of play as of 11 March 2019).

48 Belgium, Poland, Romania and Slovenia notified partial transposition. Greece, Cyprus and Luxemburg did not notify at all (state of play as of 11 March 2019).

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

50 Denmark, France, Croatia, Italy, Malta and Austria (state of play as of 11 March 2019).

51 Czechia, Estonia, Lithuania, Portugal and United Kingdom (state of play as of 11 March 2019).

52 Belgium, Bulgaria, Czechia, Germany, Estonia, Ireland, Greece, Spain, Cyprus, Latvia, Lithuania, Luxembourg, Hungary, the Netherlands, Poland, Portugal, Romania, Slovenia, Slovakia, Finland, Sweden and United Kingdom (state of play as of 11 March 2019).

As regards the transposition into national law of the **Data Protection Law Enforcement Directive**[53]**,** the Commission launched infringement procedures on 19 July 2018 against 19 Member States, owing to their failure to communicate the adoption of national legislation ensuring the full transposition of the Directive.[54] Currently, 17 Member States have notified full transposition and 5 Member States have notified partial transposition[55]. So far, procedures against 6 Member States have been closed[56], while 9 Member States received a reasoned opinion on 25 January 2019[57].

The Commission is expected to report on consistency of identification of operators of essential services by 9 May 2019. Based on the Member States' notifications, it was established that the **Directive on the security of network and information systems**[58] has been fully transposed in 25 Member States and partially transposed in one Member State.[59] In January 2019, the Commission closed infringement procedures for non-communication against 6 Member States[60]. 9 Member States[61] are subject to an infringement procedure for non-communication of full transposition of the Directive. As part of the transposition of the Directive on the security of network and information systems, Member States had to submit to the Commission by 9 November 2018 information about the operators of Essential Services identified within their territory. The Commission is now assessing the information submitted by the Member States.[62]

Moreover, the Commission is assessing the transposition of the **4th Anti-Money Laundering Directive**[63], while also working so as to verify that the rules are implemented by Member States. The Commission has launched infringement procedures against all 28 Member States as it assessed that the communications received from the Member States do not represent a

---

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

54 Belgium, Bulgaria, Czechia, Estonia, Greece, Spain, France, Croatia, Cyprus, Latvia, Lithuania, Luxembourg, Hungary, the 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 (state of play as of 11 March 2019).

55 Belgium, Germany, Estonia, Ireland, France, Croatia, Italy, Lithuania, Luxembourg, Hungary, Malta, Austria, Poland, Romania, Slovakia, Sweden and the United Kingdom notified full transposition. Czechia, Portugal, Finland, Slovenia and the Netherlands notified partial transposition. In addition, Denmark completed the transposition (state of play as of 11 March 2019).

56 Belgium, France, Croatia, Lithuania, Luxembourg, Hungary (state of play as of 11 March 2019).
Greece, Cyprus, Spain, Slovenia, Portugal, Czechia, Bulgaria, Latvia and the Netherlands (state of play as of 11 March 2019).

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

59 Bulgaria, Czechia, Denmark, Germany, Greece, Estonia, Ireland, Spain, France, Croatia, Italy, Cyprus, Latvia, Lithuania, Malta, the Netherlands, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Finland, Sweden and the United Kingdom notified full transposition. Hungary notified partial transposition. Belgium and Luxemburg did not notify any national transposition measure to the Commission (state of play as of 11 March 2019).

60 Ireland, Spain, France, Croatia, the Netherlands and Portugal (state of play as of 11 March 2019).

61 Bulgaria, Belgium, Denmark, Latvia, Lithuania, Luxemburg, Hungary, Austria and Romania (state of play as of 11 March 2019).

62 Bulgaria, Cyprus, Czechia, Germany, Denmark, Estonia, Spain, Finland, France, Croatia, Hungary, Ireland, Italy, Lithuania, Malta, the Netherlands, Poland, Portugal, Slovakia, Sweden and the United Kingdom (state of play as of 11 March 2019).

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

complete transposition of this Directive.[64] It will continue to use its powers when appropriate to ensure full implementation of this Directive.

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:

- the **EU Passenger Name Record Directive**, where 3 Member States still need to notify transposition into national law and 2 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 notify transposition into national law and 1 Member State needs to complete the notification of transposition;[66]
- the **Directive on combating terrorism**, where 3 Member States still need to notify transposition into national law and 4 Member States need to complete the notification of transposition;[67]
- the **Directive on the control of the acquisition and possession of weapons**, where 17 Member States still need to notify transposition into national law and 5 need to complete the notification of transposition;[68]
- the **Data Protection Law Enforcement Directive**, where 5 Member States still need to notify transposition into national law and 5 Member States need to complete the notification of transposition;[69] and
- the **4th Anti-Money Laundering Directive**, where 1 Member State still needs to complete the notification of transposition.[70]

64 The Commission has launched infringement procedures against all Member States for failing to communicate the national legislation fully transposing the Directive as according to the assessment, the Commission concluded that some provisions of the Directive had not been transposed.

65 Spain, the Netherlands, and Finland are yet to communicate transposition. Czechia and Slovenia communicated partial transposition and are yet to complete the notification of transposition (state of play as of 11 March 2019). 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.

66 Belgium and Luxembourg are yet to communicate transposition. Hungary communicated partial transposition and is yet to complete the notification of transposition (state of play as of 11 March 2019).

67 Greece, Cyprus and Luxembourg are yet to communicate transposition. Belgium, Poland, Romania and Slovenia communicated partial transposition and are yet to complete the notification of transposition (state of play as of 11 March 2019).

68 Belgium, Bulgaria, Germany, Ireland, Greece, Spain, Cyprus, Latvia, Luxembourg, Hungary, the Netherlands, Poland, Romania, Slovenia, Slovakia, Finland and Sweden are yet to communicate transposition. Czechia, Estonia, Lithuania, Portugal and the United Kingdom communicated partial transposition and are yet to complete the notification of transposition (state of play as of 11 March 2019). 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.

69 Bulgaria, Greece, Spain, Cyprus and Latvia are yet to communicate transposition. Czechia, Portugal, the Netherlands, Finland and Slovenia communicated partial transposition and are yet to complete the notification of transposition (state of play as of 11 March 2019).

70 Romania so far communicated only partial transposition and is yet to complete the notification of transposition. All remaining Member States have notified full transposition. However, according to the Commission assessment there are still certain provisions of the Directive regarding which the transposition does not seem to have been fully completed (state of play as of 11 March 2019).

2. Protecting public spaces: Recommended good practices

As part of the practical work to improve protection and resilience against terrorism, the Commission continues to support Member States and their local authorities in **the protection of public spaces**. Implementing the October 2017 Action Plan to support the protection of public spaces,[71] the work focuses on developing and gathering guidance and good practices. Working together with public authorities and private operators of public spaces in the so-called Operators' Forum[72], the Commission has identified good practices for several measures that all operators and public authorities involved in the protection of public spaces can implement to strengthen security.[73] They provide the basic steps to guide future work within all relevant sectors for the protection of public spaces (see box below).

Good practices for public authorities and private operators to strengthen the security of public spaces

Assessment and planning

- Establish and undertake vulnerability assessments to identify potential vulnerabilities against attacks by outsiders or insiders;
- Develop and implement a facility or event security plan, including preparatory, emergency and recovery measures, identifying the appropriate security measures for the facility's or event's environment. Security measures need to be effective, discreet, proportionate and tailor made for different environments, taking into account their specific functioning;
- Appoint and train a person responsible for the coordination and implementation of security measures contained in the security plan; and
- Develop and implement a crisis management plan.

Awareness and training

- Initiate public awareness campaigns on reporting of suspicious behaviour and how to react in the case of an attack compromising the security of a facility or event;
- Develop and implement an internal security awareness programme for all employees;
- Develop and implement an internal insider threats awareness programme that will help protect facilities or events against different types of insider threats, such as sabotage, commercial theft, or terrorist attacks;
- Develop basic security training programmes for all staff and undertake specific security trainings, contributing to the development of a corporate security culture. Develop activities that motivate employees to implement sound security practices and keep a high level of security vigilance; and
- Undertake regular security exercises that will help to identify the level of preparedness to deter and respond to an attack.

Physical protection

71 COM(2017) 612 final (18.10.2017).

72 The public-private Operators Forum, established under the October 2017 Action Plan to support the protection of public spaces, brings together Member States' policy makers and operators from different sectors, such as mass events and entertainment, hospitality, shopping malls, sports and cultural venues, transport hubs and others.

73 For further details on the good practices, see the Commission staff working document on "Good practices to support the protection of public spaces" (SWD(2019) 140 (20.3.2019)).

- Assess security and physical protection issues from the beginning of the design process of a new facility or event;
- Assess the necessary access controls and barriers, whilst avoiding to create new vulnerabilities. Access controls and barriers should not shift risks and create new targets;
- Assess the most appropriate detection technology for explosives, firearms, bladed arms, as well as chemical, biological, radiological and nuclear agents.

Cooperation

- Appoint contact points and clarify respective roles and responsibilities in public-private cooperation on security matters (e.g. between operators, private security and law enforcement authorities) and for a better communication and cooperation on a regular basis;
- Establish trustful and timely communication and cooperation that allows for a specific risk and threat information exchange between responsible public authorities, local law enforcement and the private sector;
- Coordinate the work on protection of public spaces at local, regional and national level and engage in communication and good practice exchanges at all levels including at EU level; and
- Public authorities, together with operators, should develop and make available practical recommendations and guidance materials to detect, mitigate or respond to security threats.

3. Vulnerabilities of digital infrastructures

Digital resilience is crucial for protecting the broader business of our governments, industrial research, intellectual property, business plans, our elections, democratic institutions as well as our own personal data. One of the key issues of cybersecurity receiving widespread attention in the public debate across the EU concerns 5th generation networks (5G). At the recent Telecoms informal ministerial Council in Bucharest on 1 March 2019, ministers expressed support for a coordinated European approach to strengthen digital resilience in the EU in relation to 5G networks. 5G networks infrastructure is an important basis for the digital economy. Beyond consumer services, 5G technology is designed and expected to provide mission-critical services for vertical sectors, such as mobility, energy and health. 5G networks standards are global and equipment and devices will be offered by a number of global suppliers.

The rollout of 5G networks over the next years marks a step change from earlier networks. The storing of data in the cloud will enable billions of Internet of Things devices to become connected, and power new innovations within artificial intelligence, opening up opportunities for citizens and businesses. Therefore, cybersecurity is of particular importance as vulnerabilities could be exploited, potentially causing very serious damage. Given that the Internet is borderless, a security breach in one Member State could impact on many others.

To safeguard against potential serious security implications for critical digital infrastructure, a common EU approach to the security of 5G networks is needed. To kickstart this, the Commission will issue a recommendation following the European Council of 21 and 22 March 2019 for a common EU approach to security risks to 5G networks, building on a coordinated EU risk assessment and risk-management measures, an effective cooperation and exchange of information framework, and joint EU situational awareness covering critical communication networks. The discussion on potential measures should include the

deployment of quantum technologies for network security as well as for the protection of stored data.[74]

On 12 March 2019, the European Parliament adopted a Resolution on security threats connected with the rising Chinese technological presence in the EU and possible action at EU level to reduce them.

4. External

The negotiations between the EU and Canada on a **revised Passenger Name Record Agreement** are advancing well. The upcoming EU-Canada Summit in Montreal on 11-12 April 2019 could provide positive momentum to the negotiations.

The Commission is working with United States authorities to prepare the upcoming joint evaluation of the **EU-US Passenger Name Record Agreement**[75], in line with the provisions of the EU-US Passenger Name Record Agreement. Work is already underway in the fifth joint review of the **EU-US Terrorist Finance Tracking Programme Agreement**[76]. Reviewing the safeguards, controls and reciprocity provisions of the Agreement, the joint review will also serve to assess the value of the programme as a counter-terrorism tool to both the EU and the United States.

The ongoing developments on the ground in Syria have brought into sharper focus the discussion as regards **foreign terrorist fighters** currently present or detained in conflict zones. The EU can provide support to the Member States where requested, notably as regards information exchange and support to criminal investigations, in particular cooperation with international partners and through Europol, as well as on the basis of the expertise and best practices on rehabilitation and reintegration developed in the context of the Radicalisation Awareness Network. The EU can also provide capacity-building support to third countries particularly affected by foreign terrorist fighter returnees. The decision on whether to repatriate foreign terrorist fighters and their families from conflict zones is to be taken by the Member States concerned.

The EU and Egypt co-chaired the **Global Counter Terrorism Forum** East Africa Working Group Plenary meeting in Nairobi on 20 February 2019 that saw a high rate of participation from the judiciary and police sectors of Somalia, Kenya, Sudan, Uganda, Djibouti, Somalia, Ethiopia, Yemen and Tanzania.

V. CONCLUSION

The EU has made considerable progress in the joint work towards an effective and genuine Security Union, with a number of priority legislative initiatives adopted by the European Parliament and the Council over recent weeks and months. However, there is a need for further efforts ahead of the European Parliament elections in May 2019 to address urgent security requirements. Notably, the Commission calls on the co-legislators to enter into negotiations on the proposed rules for the removal of terrorist content online as soon as the European Parliament adopted its negotiating mandate, with a view to reaching agreement still

---

74 See also the Communication on the European Cloud Initiative - Building a competitive data and knowledge economy in Europe (COM(2016) 178 final (19.4.2016)).

75 OJ L 215, 11.8.2012, p. 5.

76 OJ L 195, 27.7.2010, p. 5.

during this mandate of the European Parliament. On the proposal to strengthen the European Border and Coast Guard, negotiations are already at the trilogue stage, showing that all institutions are committed towards adopting this proposal before the European Parliament elections. The Commission also calls on Member States to implement all agreed measures in the Security Union to ensure they have full effect for the security of all citizens.

Moreover, given the time pressure to ensure the Union's preparedness before European voters go the polls in May 2019, the Commission calls on all actors involved to redouble their efforts to step up electoral resilience to counter disinformation. Ahead of the European Council on 21 and 22 March 2019, there is a need for Member States to step up their coordination and information exchange to counter disinformation and protect elections against other cyber-enabled threats, making full use of the tools the EU provides to that end. At the same time, online platforms need to accelerate their efforts across all Member States to help ensure the integrity of the European Parliament elections in May 2019. The Commission will continue to support and encourage this work in the weeks and months to come to protect the integrity of the European Parliament elections.