EUROPEAN
COMMISSION

Brussels, 30.10.2019
COM(2019) 552 final

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

Twentieth Progress Report towards an effective and genuine Security Union

I. INTRODUCTION

This is the twentieth report on the further progress made towards building an effective and genuine Security Union and covers developments under two main pillars: tackling terrorism and organised crime and the means that support them; and strengthening our defences and building resilience against those threats.

The Juncker Commission made security a top priority from day one. Building on the April 2015 European Agenda on Security[1] and the April 2016 Communication paving a way towards an effective and genuine Security Union[2], the EU responded with a coordinated approach to a series of terrorist attacks and other growing security challenges, making significant progress in enhancing our collective security.[3] It has become increasingly clear that today's security challenges – whether it is terrorism, organised crime, cyberattacks, disinformation or other evolving cyber-enabled threats – are shared threats. Only by working together can we achieve the level of collective security that citizens rightly demand and expect. This shared understanding has been the basis for the progress made towards an effective and genuine Security Union. Driven by the needs of national authorities working on keeping citizens safe, the EU-level support has focused on legislative and operational measures where joint action can have an impact on the security of Member States. This work has been carried out in close conjunction with the European Parliament and the Council, and with full transparency towards the wider public. Full respect of fundamental rights has been at the heart of this work, as the security of the Union can only be ensured when citizens are confident that their fundamental rights are fully respected.

The EU has worked to **counter terrorism** by closing down the space in which terrorists operate, with new rules making it harder for them to access explosives, firearms and financing, and to restrict their movements. The EU has stepped up **information exchange** to provide those on the frontline, police officers and border guards, with efficient access to accurate and complete data, making best use of existing information and closing gaps and blind spots. Strong protection of the external borders is a precondition for security in the area of free movement without internal border controls. In March 2019, the European Parliament and the Council reached agreement on a further strengthened and fully equipped **European Border and Coast Guard** and the new Regulation is expected to enter into force in early December 2019. The EU has provided a platform and funding for those working in local communities to exchange best practices on **countering radicalisation and preventing violent extremism**, as well as proposing new rules to effectively remove terrorist content online. EU support has helped **make cities more resilient** against attacks, with action plans to support the protection of public spaces and to enhance preparedness against chemical, biological, radiological and nuclear security risks. The EU has addressed **cybersecurity and cyber-enabled threats**, by putting in place a new EU cybersecurity strategy and adopting relevant legislation, and tackling **disinformation** to better protect our elections. Work continues to strengthen the security of our **digital critical infrastructure**, including reinforced cooperation on the **cybersecurity of 5G networks** across Europe.

More still remains to be done. The live-streamed attack against a synagogue and the killing of

[1] COM(2015) 185 final (28.4.2015).
[2] COM(2016) 230 final (20.4.2016).
[3] For previous progress reports towards an effective and genuine Security Union see: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

two citizens in Halle, Germany on 9 October 2019 was a shocking reminder of the threat posed by right-wing violent extremism and anti-Semitism. It also highlighted once again the misuse of the internet for terrorist propaganda and hence the **need for EU-wide rules for the deletion of terrorist content online**. The 7-8 October 2019 Justice and Home Affairs Council debated right-wing violent extremism and terrorism, stressing the need for further work including on countering the spread of unlawful right-wing extremist content online and offline. At the same time, the killing of three police officers and another staff member in the Paris police headquarters on 3 October 2019 shows that the threat from jihadi inspired terrorism remains real, and that on-going efforts to support Member States in addressing this threat need to continue. The escape of imprisoned members of ISIS/Da'esh in the context of recent events in Northern Syria could have a serious impact on security in Europe. It is important that Member States make full use of existing information systems to detect and identify foreign terrorist fighters when crossing the external borders. Work is also on-going on the use of battlefield information to prosecute foreign terrorist fighters.

This report sets out the recent progress made in the work towards an effective and genuine Security Union, highlighting areas where further action is needed. It provides an update on the implementation of agreed measures on **cybersecurity of 5G networks**, in particular on the **EU Risk Assessment Repor**t published on 9 October 2019, and on **countering disinformation**.

This report focuses in particular on the **external dimension** of the cooperation in the Security Union, with the signing of two bilateral **counter-terrorism arrangements** with Albania and the Republic of North Macedonia and progress made in the cooperation with third country partners on the exchange of **passenger name record data**. In addition, together with this report, the Commission adopted a request for authorisation for the launch of negotiations for an agreement between the EU and **New Zealand** on the exchange of personal data to fight serious crime and terrorism.

II. DELIVERING ON LEGISLATIVE PRIORITIES

1. Preventing radicalisation online and in communities

The **prevention of radicalisation** is a cornerstone of the Union's response to the threats posed by terrorism. In that respect, the internet has been the most significant battleground for terrorists' action in the 21st century. Spaces in which radicalised individuals can communicate and share content enable the development of worldwide, expanding networks of both jihadi and right-wing violent extremists. This is why the Commission continues its two-track approach against online radicalisation where proposed rules on removing illegal terrorist content online should reinforce the voluntary partnership with online platforms.

Essential to this is the **legislative proposal to prevent the dissemination of terrorist content online**, with clear rules and safeguards that would make it mandatory for internet platforms to take down terrorist content within one hour upon receipt of a reasoned request by competent authorities, and to take proactive measures proportionate to the level of exposure to terrorist content.[4] Interinstitutional negotiations are ongoing between the European Parliament and the Council, with a first trilogue meeting held on 17 October 2019. Given the threat posed by terrorist content online, the Commission calls on the co-legislators to reach agreement on

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

the proposed legislation by the end of 2019.

The proposed legislation complements the voluntary partnership with the internet industry and other stakeholders taking place in the **EU Internet Forum**. Since its creation in 2015, it has been a catalyst for internet companies to act proactively to identify and remove terrorist content online, paving the way for the industry-led initiative of a 'shared database of hashes'[5] and the creation of the Global Internet Forum to Counter Terrorism. The EU Internet Referral Unit, part of the EU law enforcement agency Europol, has been instrumental in strengthening cooperation with internet companies and contributing to the overall objectives of the EU Internet Forum. At the latest Ministerial meeting of the EU Internet Forum on 7 October 2019, EU Member States and senior representatives of internet companies committed to collaborating under the so-called **EU Crisis Protocol**. The EU Crisis Protocol identifies thresholds for enhanced cooperation and establishes new ways to enhance crisis response. This is part of the efforts at international level to implement the 'Christchurch Call for Action'[6], seeking to ensure coordinated and rapid reaction to contain the spread of viral terrorist or violent extremist content online.

Beyond those measures against online radicalisation, the Commission continues to support efforts at national and local level to **prevent and counter radicalisation on the ground**. Building on the wealth of experience and expertise gathered within the Radicalisation Awareness Network, the EU offers targeted support to local actors including cities[7], and provides opportunities for exchange between practitioners, researchers and policy makers. For example, the network has issued specific guidance and organised workshops to support competent authorities in dealing with children who came from conflict zones.[8] To ensure the continuity of activities carried out within the Radicalisation Awareness Network, the Commission has launched the procedure for a new framework contract for an estimated value of EUR 61 million over a period of four years, starting in 2020.[9]

In order to counter the threat posed by terrorist content online, the Commission calls on the European Parliament and the Council:
• to conclude the negotiations on the legislative proposal to prevent the dissemination of **terrorist content online** before the end of the year.

5 A tool set up by a consortium of companies to facilitate co-operation so as to prevent the dissemination of terrorist content across platforms.

6 In response to the attacks in Christchurch, New Zealand on 15 March 2019, French President Emmanuel Macron and New Zealand's Prime Minister Jacinda Ardern invited Leaders and online platforms to Paris on 15 May 2019 to launch the 'Christchurch Call to Action'. President Juncker supported the call and announced the development of an EU crisis protocol.

7 For the cooperation with cities on security, see also section V.2 on preparedness and protection and notably on the protection of public spaces.

8 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_child_returnees_from_conflict_zones_112016_en.pdf

9 The framework contract is split in two lots: EUR 29.000.000 to support the activities of the Radicalisation Awareness Network for the next four years and EUR 32.000.000 to enhance the capabilities of Member States, national, regional and local authorities and priority third countries in effectively tackling radicalisation in particular by offering networking opportunities, targeted and needs driven services and research and analysis.

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

The EU has stepped up information exchange, making it easier to tackle identity fraud[10], strengthening border checks[11], modernising Europe-wide law enforcement databases[12], closing information gaps[13] and reinforcing the EU law enforcement agency Europol[14]. Central to this is the **interoperability of EU information systems**[15], which means making best use of existing information and closing blind spots. Responding to the needs of those working on the frontline, interoperability will lead to faster, more systematic access to information for law enforcement officers, border guards and migration officials, thus contributing to improving internal security and border management.

However, interoperability and all the innovation it entails will only make a difference for security, border and migration management on the ground if each Member State fully implements the related legislation. This is why the **implementation** of interoperability is a top priority in the Security Union, both at political and technical levels. The Commission and the EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) support Member States with expertise and the exchange of best practices, using a network of national coordinators and developing a scorecard to enable effective monitoring and coordination arrangements. Close cooperation between EU agencies, all Member States and Schengen associated countries will be paramount in order to attain the ambitious objective of achieving full interoperability of EU information systems for security, border and migration management by 2020.

Meanwhile, the European Parliament and the Council are still to **complete the legislative work** in this respect. Swift agreement on all pending legislative proposals is essential to secure complete and timely roll-out of interoperability. First, as part of the technical

---

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

11 Introduction of systematic checks carried out at the external borders on all citizens using the Schengen Information System. All Schengen States, as well as Romania, Bulgaria, Croatia and Cyprus, apply the rules on systematic checks against relevant databases at external borders, as introduced in April 2017. In line with these rules, temporary derogations are possible at land or sea borders but only with regard to EU citizens, in view of the disproportionate impact on the flow of traffic. Currently, such derogations have been notified by six Member States/Schengen Associated Countries (Croatia, Finland, Hungary, Latvia, Norway and Slovenia). As regards air borders, the possibility of derogating from the rules on systematic checks expired in April 2019.

12 The reinforced Schengen Information System (Regulation (EU) 2018/1860 (28.11.2018), Regulation (EU) 2018/1861 (28.11.2018), Regulation (EU) 2018/1862 (28.11.2018)) and the European Criminal Records Information System extended to third-country nationals (Regulation (EU) 2019/816 (17.4.2019)). The strengthening of the Schengen Information System includes a general obligation to enter terrorism-related alerts in the system.

13 The EU Entry/Exit System (Regulation (EU) 2017/2226 (30.11.2017)) and the European Travel Information and Authorisation System (Regulation (EU) 2018/1240 (12.9.2018) and Regulation (EU) 2018/1241 (12.9.2018)).

14 Over the last years Europol's role has been considerably reinforced both in scope and depth. The Agency has been strengthened with the adoption of the Europol Regulation in 2016 (Regulation (EU) 2016/794 (11.5.2016). Member States have significantly increased the amount of information shared with and via Europol. The establishment of the Europol Counter Terrorism Centre (ECTC) has strengthened Europol's analytical capabilities in terrorism cases. Europol's budget consistently increased over the last years, from EUR 82 million in 2014 to EUR 138 million in 2019. Negotiations on the budget for 2020 are ongoing.

15 Regulation (EU) 2019/817 (20.5.2019) and Regulation (EU) 2019/818 (20.5.2019).

implementation of the **European Travel Information and Authorisation System**, there is a need for technical amendments to the related Regulations[16] to fully set up the system. The Commission invites the European Parliament to speed up its work on these technical amendments in order to start interinstitutional negotiations as soon as possible. Second, interinstitutional negotiations are still on-going on the May 2018 proposal to strengthen and upgrade the existing **Visa Information System**.[17] Building on the first trilogue meeting that took place on 22 October 2019, the Commission calls on both co-legislators to swiftly conclude the negotiations. Third, agreement is still pending on the May 2016 Commission proposal to extend the scope of **Eurodac**[18] by storing not only the fingerprints and relevant data of asylum applicants and of persons apprehended in connection to an irregular crossing of the external border, but also those of illegally-staying third-country nationals. The proposed changes would also extend the storage period of fingerprints and relevant data of those who enter the EU irregularly. The Commission calls on the co-legislators to proceed to the adoption of the proposal.

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 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**.
- to swiftly conduct and conclude negotiations on the proposal to strengthen the existing **Visa Information System**.
- to adopt the legislative proposal on **Eurodac** *(Joint Declaration priority).*

3. Closing down the space in which terrorists operate

The EU has taken firm action to close down the space in which terrorists operate, with new rules making it harder for terrorists and other criminals to access explosives[19], firearms and financing[20], and to restrict their movement.[21]

To strengthen the judicial response to terrorism, the EU Agency for Criminal Justice Cooperation (Eurojust) set up on 1 September 2019 a **European Judicial Counter Terrorism Register**. The register will gather judicial information to establish links in proceedings against suspects of terrorist offences, thus reinforcing coordination among prosecutors in counter-terrorism investigations with potential cross-border implications.

Further efforts are needed, however, to support and facilitate investigations in cross-border cases, notably when it comes to law enforcement **access to electronic evidence**. As regards the April 2018 legislative proposals to improve cross-border access to electronic evidence in criminal investigations[22], the European Parliament has yet to adopt its negotiating position

16 Regulation (EU) 2018/1240 (12.9.2018) and Regulation (EU) 2018/1241 (12.9.2018)
17 COM (2018) 302 final (16.5.2018).
18 COM (2016) 272 final (4.5.2016).
19 Regulation (EU) 2019/1148 (20.6.2019) on the marketing and use of explosives precursors. The Regulation entered into effect on 31 July 2019 and shall apply 18 months after its entry into force.
20 Directive (EU) 2019/1153 (11.7.2019) laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences.
21 Introduction of systematic checks carried out at the external borders on all citizens using the Schengen Information System.
22 COM(2018) 225 final (17.4.2018) and COM(2018) 226 final (17.4.2018).

before the co-legislators can enter into negotiations. The Commission urges the European Parliament to advance on this legislative proposal so that the co-legislators can work towards swift adoption. On the basis of its proposal for EU-internal rules, the Commission is also engaging in **international negotiations** to improve cross-border access to electronic evidence. On 25 September 2019, the Commission and United States authorities held the first formal negotiation round on an **EU-US Agreement on cross-border access to electronic evidence**. A further round is scheduled for 6 November 2019. In the context of the ongoing negotiations of a **Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime**, the Commission participated on behalf of the Union in three negotiating sessions in July, September and October 2019. While good progress has been made in these negotiations, a number of major topics of significant interest to the Union are still to be addressed, such as data protection safeguards. The negotiation of a Second Additional Protocol will continue in November 2019 and throughout 2020. It is important to proceed fast with both 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.

Reflecting on-going concerns about money laundering, the European Parliament adopted on 19 September 2019 a **Resolution on the state of implementation of the Union's anti-money laundering legislation**[23], responding to the package of four reports on anti-money laundering that the Commission adopted on 24 July 2019[24]. The European Parliament called on Member States to ensure the proper and speedy implementation of anti-money laundering directives. The European Parliament also called on the Commission to assess whether an anti-money laundering regulation would be more appropriate than a Directive and to assess the need for a coordination and support mechanism for financial intelligence units.

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

- to reach swift agreement on the legislative proposals on **electronic evidence** *(Joint Declaration priority).*

4. Enhancing cybersecurity

Enhancing cybersecurity remains a key aspect of the work towards a genuine and effective Security Union. Implementing the 2017 EU Cybersecurity Strategy[25], the Union has strengthened its resilience by making itself harder to attack and quicker to recover, as well as its deterrence by increasing the chances of attackers getting caught and punished, including through a framework for a joint EU diplomatic response to malicious cyber activities. The

[23] https://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_EN.html

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

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

Union also supports Member States in cyber defence, implementing the EU Cyber Defence Policy Framework.[26]

With the entry into force of the Cybersecurity Act[27] in June 2019, the **EU cybersecurity certification framework** is taking shape. Certification plays a critical role in increasing trust and security in products and services that are crucial for the Digital Single Market. The certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. It involves two expert groups, namely the European Cybersecurity Certification Group representing Member State authorities and the Stakeholder Cybersecurity Certification Group representing industry. The latter brings together both the demand and supply side of information and communication technology products and services, including small and medium-sized enterprises, digital service providers, European and international standardisation bodies, national accreditation bodies, data protection supervisory authorities and conformity assessment bodies.

Meanwhile, the European Parliament and the Council still have to reach agreement on the legislative initiative[28] for a **European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres**. The proposal aims to strengthen the Union's cybersecurity capacity by stimulating the European technological and industrial cybersecurity ecosystem as well as coordinating and pooling related resources. The Commission calls on both co-legislators to resume and swiftly conclude interinstitutional negotiations on this priority initiative to enhance cybersecurity.

The work to enhance cybersecurity includes support for both the national and regional levels.[29]

Beyond cyber threats targeting systems and data, the EU continues to address the complex and multifaceted challenges posed by **hybrid threats**. In the Council, a horizontal working party on countering hybrid threats has been established to improve the resilience of the EU and its Member States against hybrid threats and to support action to strengthen the crisis resilience of societies. The Commission and the European External Action Service support these efforts under the 2016 Joint Framework on Countering Hybrid Threats[30] and the 2018 Joint Communication[31] on increasing resilience and bolstering capabilities to address hybrid threats. Moreover, the Joint Research Centre is elaborating a 'conceptual model' framework to characterise hybrid threats, with the aim to help Member States and their competent authorities to identify the type of hybrid attack they might face. The model looks at the way in which an actor (state or non-state) employs a series of tools (from disinformation to espionage or physical operations) in various domains (economic, military, social, political) to affect a target in order to achieve a series of objectives.

---

26 EU Cyber Defence Policy Framework (2018 update) as adopted by the Council on 19 November 2018 (14413/18).

27 Regulation (EU) 2019/881 (17.4.2019.

28 COM(2018) 630 final (12.9.2018).

29 For example, the Commission supports an interregional innovation partnership on cybersecurity involving Brittany, Castilla y León, Nordrhein-Westfalen, Central Finland and Estonia to develop a European cybersecurity value chain with a focus on commercialisation and scaling-up.

30 JOIN(2016) 18 final (6.4.2016).

31 JOIN(2018) 16 final (13.6.2018).

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

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

III. ENHANCING THE SECURITY OF DIGITAL INFRASTRUCTURES

Fifth Generation (5G) networks will be the future backbone of increasingly digitised economies and societies. Billions of connected objects and systems are concerned, including in critical sectors such as energy, transport, banking, and health, as well as industrial control systems carrying sensitive information and supporting safety systems. Ensuring the cybersecurity and resilience of 5G networks is therefore essential.

As part of a coordinated approach, Member States published on 9 October 2019 a report on the **EU coordinated risk assessment on cybersecurity in 5G networks** with the support of the Commission and the European Agency for Cybersecurity.[32] This major step is part of the implementation of the March 2019 Commission Recommendation to ensure a high level of cybersecurity of 5G networks across the EU.[33] The report is based on the results of the national cybersecurity risk assessments by all Member States. It identifies the main threats and threat actors, the most sensitive assets, the main vulnerabilities (including technical ones and other types of vulnerabilities) and a number of strategic risks. This assessment provides the basis to identify mitigation measures that can be applied at national and European level.

The report identifies a number of important **cybersecurity challenges** which are likely to appear or become more prominent in 5G networks. These security challenges are mainly linked to key *innovations* in 5G technology, in particular the importance of software and the wide range of services and applications enabled by 5G, as well as the role of *suppliers* in building and operating 5G networks and the degree of dependency on individual suppliers. This means that suppliers' products, services and operations increasingly become part of the 'attack surface' of 5G networks. Moreover, the risk profile of individual suppliers will become particularly important, including the likelihood of the supplier being subject to interference from a non-EU country.

In line with the process set out in the March 2019 Commission Recommendation, Member States should agree by 31 December 2019 on a **toolbox of mitigating measures** to address the identified cybersecurity risks at national and Union level. The Commission and the European External Action Service will also continue to exchange with like-minded partners about cybersecurity and resilience of 5G networks. In that respect, the Commission is in contact with NATO on the EU coordinated risk assessment of the cybersecurity of 5G networks.

---

[32] The EU coordinated risk assessment on cybersecurity in 5G networks was completed by the Cooperation Group of competent authorities as set out under the Directive on Security of Network and Information Systems (Directive (EU) 2016/1148 (6.7.2016), with the help of the Commission and the European Agency for Cybersecurity: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[33] C(2019)2355 final (26.3.2019).

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

The EU has established a **framework for coordinated action against disinformation**, with full respect for European values and fundamental rights.[34] Under the Action Plan against Disinformation[35], work continues to close down the space for disinformation, including with a view to protect the integrity of elections.

Central to this is the work with industry through the self-regulatory **Code of Practice on Disinformation** for online platforms and the advertising sector that became applicable in October 2018.[36] The Commission has assessed the effectiveness of the Code following its first year of operations, based on annual self-assessment reports submitted by the online platforms and the other Code signatories and published on 29 October 2019 together with a Commission Statement.[37] Broadly, the reports demonstrate serious efforts by the signatories to implement their commitments.

Actions taken by the platforms signatories vary in terms of speed and scope across the Code's five pillars of commitments. In general, progress is more advanced with respect to commitments relating to the 2019 European election, namely on disrupting advertising and monetisation incentives for disinformation (pillar 1), ensuring the transparency of political and issue-based advertising (pillar 2), and ensuring the integrity of services against inauthentic accounts and behaviours (pillar 3). By contrast, progress is less advanced or lacking with respect to commitments to empower consumers (pillar 4) and commitments to empower the research community, including via the provision by platforms of relevant and privacy-compliant access to datasets for research purposes (pillar 5). There are also differences in the scope of actions undertaken by each platform to ensure the implementation of their commitments as well as differences across Member States as regards the deployment of the individual policies. The Commission continues to work with Code signatories and other stakeholders to step up the action taken against disinformation.

Under the Action Plan against Disinformation, the Commission and the High Representative, in cooperation with the Member States, set up a **Rapid Alert System** for addressing disinformation campaigns. The Rapid Alert System enabled EU Institutions and Member States to share information and analyses ahead of the 2019 elections to the European Parliament, and to coordinate responses. This work has intensified further after the elections, with working-level exchanges ongoing on a daily basis and three meetings of the Rapid Alert Systems Points of Contact organised by different Member States.

---

34 See the Action Plan against Disinformation (JOIN(2018) 36 final (5.12.2018)).

35 JOIN (2019) 12 final (14.6.2019).

36 Under the Code, the online platforms Google, Facebook, Twitter, and Microsoft have committed to prevent the manipulative use of their services by bad actors, provide for the transparency and public disclosure of political advertising, and take other actions to improve the transparency, accountability and trustworthiness of the online ecosystem. Trade associations from the advertising sector have also committed to cooperating with the platforms to improve the scrutiny of ad placements and develop brand safety tools aimed at limiting the placement of advertising on websites that purvey disinformation.

37 https://ec.europa.eu/commission/presscorner/detail/en/statement_19_6166. In addition to Google, Facebook, Twitter and Microsoft, the other signatories to the Code include Mozilla, seven European-level or national-level associations representing the advertising sector, and EDiMA, a European association representing platforms and other technology companies active in the online sector.

Another practical step to identify disinformation has come with the work of the **Strategic Communications Team** ('StratComms'), and in particular its East Stratcom Taskforce, which has been running the 'EUvsDisinfo' project to monitor, analyse and respond to pro-Kremlin disinformation.[38] Since the beginning of 2019, the first dedicated budget of EUR 3 million has made it possible to step up and expand this work to include the monitoring and analysis of pro-Kremlin disinformation in web, broadcast and social media in 19 languages ranging from English to Serbian and Arabic. The amount of exposed disinformation activities more than doubled due to improved monitoring capacity, with around 2000 disinformation cases so far in 2019 compared to 765 cases during the same period in 2018. The East Stratcom Taskforce played a vital role in monitoring and exposing pro-Kremlin disinformation targeting the 2019 elections to the European Parliament. The research was paired with a campaign to raise awareness about attempted interference in electoral processes around the world. Its outreach, carried out in close cooperation with the European Parliament and the Commission, resulted in more than 20 media interviews, while the campaign engaged more than 300 journalists.

The Commission has also taken action to **reduce the spread of disinformation and myths about EU institutions and policies**. It has established a network of communication experts with an online portal providing interactive information material on EU policies and the challenge of disinformation and its impact on society. It has also launched a series of social media campaigns focusing on tackling disinformation[39], in collaboration with the European Parliament and the European External Action Service.

V. IMPLEMENTATION OF OTHER PRIORITY FILES ON SECURITY

1. Implementation of legislative measures in the Security Union

Agreed measures in the Security Union will only bring full benefits to security if all Member States ensure their swift and complete implementation. To this end, the Commission is actively supporting Member States in the implementation of EU legislation, including through funding and by facilitating the exchange of best practices. The Commission makes full use of its powers under the Treaties for the enforcement of EU law, including infringement action as appropriate.

The deadline for the transposition of the **EU Passenger Name Record Directive**[40] expired on 25 May 2018. To date, 25 Member States have notified full transposition[41], which represents significant progress since July 2018 when the Commission launched infringement procedures against 14 Member States.[42] Two Member States have yet to notify full transposition, despite on-going infringement procedures launched on 19 July 2018.[43] 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

38 www.euvsdisinfo.eu

39 https://europa.eu/euprotects/

40 Directive (EU) 2016/681 (27.4.2016). Denmark did not take part in the adoption of this Directive and is not bound by it or subject to its application.

41 The references to full transposition notification take account of the Member States' declarations and are without prejudice to the transposition check by the Commission services (state of play as of 17.10.2019).

42 See the Sixteenth Progress Report towards an effective and genuine Security Union (COM(2018) 690 final (10.10.2018)).

43 Slovenia notified partial transposition. Spain did not notify transposition (state of play as of 17.10.2019).

practices.

The deadline for the transposition of the **Directive on combating terrorism**[44] expired on 8 September 2018. To date, 22 Member States have notified full transposition, which represents significant progress since November 2018 when the Commission launched infringement procedures against 16 Member States.[45] Three Member States have yet to notify full transposition, despite the on-going infringement procedures.[46] On 25 July 2019, the Commission sent reasoned opinions to two Member States for failing to notify full transposition of the Directive[47]. In response, both Member States announced that legislative work will be completed before the end of this year.

The deadline for the transposition of the **Directive on the control of the acquisition and possession of weapons**[48] expired on 14 September 2018. To date, 13 Member States have notified full transposition. 15 Member States have yet to notify full transposition, despite on-going infringement procedures launched on 22 November 2018.[49] On 25 July 2019, the Commission sent reasoned opinions to 20 Member States for failing to notify full transposition of the Directive. In response, five Member States notified full transposition of the Directive.[50]

The deadline for the transposition of the **Data Protection Law Enforcement Directive**[51] expired on 6 May 2018. To date, 25 Member States have notified full transposition, which represents significant progress since July 2018 when the Commission launched infringement procedures against 19 Member States.[52] Three Member States have yet to notify full transposition, despite the on-going infringement procedures.[53] On 25 July 2019, the Commission decided to refer two Member States[54] to the Court of Justice of the European Union for non-transposition of the Directive and sent a letter of formal notice to one Member State[55] for failing to fully transpose the Directive.[56]

The Commission is assessing the transposition of the **4th Anti-Money Laundering Directive**[57], while also working to verify that the rules are implemented by Member States.

---

44 Directive (EU) 2017/541 (15.3.2017). The Directive is not applicable in the United Kingdom, Ireland and Denmark.

45 See the Seventeenth Progress Report towards an effective and genuine Security Union (COM(2018) 845 final (11.12.2018)).

46 Greece and Luxembourg have not notified national implementing measures. Poland has notified national measures amounting to partial transposition (state of play as of 17.10.2019).

47 Greece and Luxembourg.

48 Directive (EU) 2017/853 (17.10.2019).

49 Belgium, Czechia, Estonia, Poland, Sweden, Slovakia, United Kingdom have notified transposition measures for part of the new provisions. Cyprus, Germany, Greece, Spain, Luxembourg, Hungary, Romania, Slovenia have not notified any transposition measures (state of play as of 17.10.2019).

50 Finland, Ireland, Lithuania, Netherlands, Portugal (state of play as of 17.10.2019).

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

52 See the Sixteenth Progress Report towards an effective and genuine Security Union (COM(2018) 690 final (10.10.2018)).

53 Slovenia notified partial transposition. Spain did not notify transposition. Although Germany notified complete transposition, the Commission considers this transposition not to be complete (state of play as of 17.10.2019).

54 Greece and Spain.

55 Germany.

56 Greece notified full transposition which the Commission is assessing.

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

They had to transpose the Directive into national law by 26 June 2018. The Commission maintains infringement procedures against 21 Member States as it assessed that the communication received from the Member States does not represent a complete transposition of this Directive.[58]

The Commission has assessed the conformity of the transposition of **cybercrime-related directives**. It has launched in July and October 2019 infringement procedures against 23 Member States[59] as it assessed that the national implementing legislation notified by those Member States did not represent a correct transposition of the **Directive on combatting child sexual abuse**[60]. The Commission has likewise initiated in July and October 2019 infringement procedures against four Member States[61] as it assessed that the national implementing legislation notified by those Member States did not represent a correct transposition of the **Directive on attacks against information systems**[62].

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 1 Member State still needs to notify transposition into national law and 1 Member State still needs to complete the notification of transposition;[63]
- the **Directive on combating terrorism**, where 2 Member States still need to notify transposition into national law and 1 Member State still needs to complete the notification of transposition;[64]
- the **Directive on the control of the acquisition and possession of weapons**, where 8 Member States still need to notify transposition into national law and 7 Member States still need to complete the notification of transposition;[65]
- the **Data Protection Law Enforcement Directive,** where 1 Member State still needs to notify transposition into national law and 2 Member States still need to complete the notification of transposition;[66]
- the **4th Anti-Money Laundering Directive**, where 21 Member States still need to complete the notification of transposition;[67]

58 Belgium, Bulgaria, Czechia, Denmark, Germany, Estonia, Ireland, France, Italy, Cyprus, Latvia, Lithuania, Hungary, Netherlands, Austria, Poland, Romania, Slovakia, Finland, Sweden and the United Kingdom (state of play as of 17.10.2019.). Previously, 7 infringement procedures related to the Directive were closed.

59 Belgium, Bulgaria, Czechia, Germany, Estonia, Greece, Spain, France, Croatia, Italy, Latvia, Lithuania, Luxembourg, Hungary, Malta, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Finland and Sweden.

60 Directive 2011/93/EU (13.12.2011).

61 Bulgaria, Italy, Portugal and Slovenia.

62 Directive 2013/40/EU (12.08.2013).

63 Slovenia notified partial transposition. Spain did not notify transposition (state of play as of 17.10.2019).

64 Greece and Luxembourg did not notify transposition. Poland notified partial transposition (state of play as of 17.10.2019).

65 Belgium, Czechia, Estonia, Poland, Sweden, Slovakia, United Kingdom have notified transposition measures for part of the new provisions. Cyprus, Germany, Greece, Spain, Luxembourg, Hungary, Romania, Slovenia have not notified any transposition measures (state of play as of 17.10.2019).

66 Slovenia notified partial transposition. Spain did not notify transposition. Although Germany notified complete transposition, the Commission considers this transposition not to be complete (state of play as of 17.10.2019.).

- the **Directive on combatting child sexual abuse,** where infringement procedures for incorrect transposition have been launched against 23 Member States;[68]
- the **Directive on attacks against information systems** where infringement procedures for incorrect transposition have been launched against 4 Member States.[69]

2. Preparedness and protection

Building resilience against security threats is an essential part of the work towards an effective and genuine Security Union. The Commission supports Member States and local authorities in enhancing the protection of public spaces, implementing the October 2017 Action Plan and the January 2019 Partnership for Security in Public Spaces under the Urban Agenda for the EU. This work involves those cities that approached the Commission and asked for support in addressing the challenges they had faced in protecting public spaces.

Exchanging best practices among local authorities and with private operators is key to strengthening the security of public spaces. This was at the heart of the **European Week of Security** in Nice, France from 14 to 18 October 2019, organised by the EU-funded project 'Protect Allied Cities against Terrorism in Securing Urban Areas'. Bringing together 500 participants from cities all over Europe, national authorities and research institutions, the event highlighted the importance of close cooperation between all stakeholders involved, both public and private, and the role of new technologies in better protecting cities. Protection of public spaces also featured in the **European Week of Regions and Cities** in Brussels from 7 to 10 October 2019, with a workshop on the Urban Agenda for the EU Partnership for Security in Public Spaces. It focused on the role of local authorities in the security policy domain, EU regulation and funding to face main security challenges in urban public spaces, and key themes such as innovation through smart solutions and technologies, including the concept of security by design, prevention and social inclusion. The Commission is also contributing to foster cities' innovation in these fields through its last call for proposals of the Urban Innovative Actions, the results of which were announced in August 2019. Among the projects selected, three cities (Piraeus in Greece, Tampere in Finland and Turin in Italy) will be testing new solutions on urban security matters.[70]

To better **protect places of worship** and to explore the needs of different religious groups, the Commission organised a meeting on 7 October 2019 with representatives of Jewish, Muslim, Christian and Buddhist communities. Part of the implementation of the 2017 EU Action Plan to support the protection of public spaces, the meeting indicated that the security awareness and preparedness vary significantly between different religious communities, highlighting the importance of further exchange of good practices. The meeting also showed that introducing basic security measures and a better security awareness are not incompatible with maintaining the open and accessible character of places of worship. The Commission will collect good practices and awareness raising material on its electronic expert platform and bring the matter

---

67 Belgium, Bulgaria, Czechia, Denmark, Germany, Estonia, Ireland, France, Italy, Cyprus, Latvia, Lithuania, Hungary, Netherlands, Austria, Poland, Romania, Slovakia, Finland, Sweden and the United Kingdom (state of play as of 17.10.2019).

68 Belgium, Bulgaria, Czechia, Germany, Estonia, Greece, Spain, France, Croatia, Italy, Latvia, Lithuania, Luxembourg, Hungary, Malta, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Finland and Sweden.

69 Bulgaria, Italy, Portugal and Slovenia.

70 The Urban Innovative Actions are an instrument co-funded by the European Regional Development. For more information see: https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals.

to the attention of Member States' security authorities in the public-private forum for the protection of public spaces.

One specific area requiring further attention is the increasing security threat to critical infrastructure and public spaces posed by **drones**. Complementing recent EU legislation[71] on safe drone operations in manned airspace, and without undermining the opportunities for the beneficial use of drones, the Commission supports Member States in tracking trends in the malicious use of drones, funding relevant research and facilitating the testing of countermeasures. Exchange of experiences and best practices are crucial, as shown by the high-level international conference on countering the threats posed by unmanned aircraft systems in Brussels on 17 October 2019. Organised by the Commission, this event brought together 250 participants from Member States, international organisations, third countries partners, industry, academia and civil society to discuss the security challenges posed by drones and ways to address them. The meeting showed a need for regular risk assessments related to drones and for close cooperation between aviation and law enforcement authorities in further developing European legislation on safe drone operations. There is also a need for further testing of countermeasures against drones through a coordinated European approach. Furthermore, there was agreement that for drones to be safe, secure, operationally reliable and difficult to misuse for malicious purposes, close engagement between authorities and industry is essential.

3. External dimension

As most of the security risks facing the Union go beyond EU borders and represent global threats, cooperation with partner countries, organisations and relevant stakeholders plays a vital role in building an effective and genuine Security Union.

Information exchange is central to this cooperation. Together with this report, the Commission adopted a recommendation to the Council for authorising the opening of negotiations for an **agreement between the EU and New Zealand on the exchange of personal data for fighting serious crime and terrorism** between Europol and New Zealand competent authorities. Such agreement will further strengthen Europol's capabilities to engage with New Zealand for the purposes of preventing and combatting crimes falling within the scope of Europol's objectives. While the April 2019 working arrangement between Europol and New Zealand Police provides a framework for structured strategic-level cooperation, it does not provide a legal basis for the exchange of personal data. Exchanging personal data in full respect of EU law and fundamental rights is essential for effective operational police cooperation. Previously, the Commission identified eight priority countries in the Middle East/North Africa Region on the basis of the terrorist threat, migration-related challenges and Europol's operational needs to start negotiations.[72] Taking into account the operational needs of law enforcement authorities across the EU, and the potential benefits of closer cooperation in this area as also demonstrated by the follow up to the Christchurch attack of March 2019, the Commission considers it necessary to add New Zealand as a priority country to start negotiations with in the short-term.

---

71 Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft systems.

72 See the Eleventh Progress Report towards an effective and genuine Security Union (COM(2017) 608 final (18.10.2017). The priority countries are Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey.

Another cornerstone of the Union's security cooperation with third country partners is the transfer of **passenger name record data**. On 27 September 2019, the Commission adopted a Recommendation to the Council to authorise the opening of negotiations for an **EU-Japan** agreement on the transfer of passenger name record data in order to prevent and combat terrorism and serious transnational crime in full respect of data protection safeguards and fundamental rights.[73] The recommendation is being examined at Council working group level and the Commission calls on the Council to adopt swiftly a mandate for negotiations with Japan. Having arrangements in place in time for the 2020 Olympics would bring a real security dividend.

On the global level, the Commission supports the work carried out by the **International Civil Aviation Organisation** to establish a standard for processing passenger name record data. This responds to a call by United Nations Security Council Resolution 2396 that urges all United Nations Member States to develop the capability to collect, process and analyse passenger name record data. On 13 September 2019, the Commission presented a proposal[74] for a Council Decision on the position to be taken on behalf of the EU in the International Civil Aviation Organization with regard to standards and recommended practices on passenger name record data. The proposal is being examined at Council working group level and the Commission calls for swift adoption of the Council Decision. The position of the Union and its Member States has also been set out in an information paper on 'Standards and principles on the collection, use, processing and protection of Passenger Name Record data' that was submitted to the 40th Session of the International Civil Aviation Organisation Assembly.

As regards the work towards a new passenger name record agreement with **Canada**, the Commission seeks swift finalisation of the agreement. Meanwhile, the combined joint review and joint evaluation of the passenger name record agreement with **Australia** as well as the joint evaluation of the passenger name record agreement with the **United States** were launched this summer, starting with visits to Canberra and Washington in August and September 2019 respectively. The Commission informed the European Parliament's Committee on Civil Liberties, Justice and Home Affairs in a closed session on 14 October 2019 about the state of play of the work with Japan, Australia and Canada on passenger name record data.

There is also progress in security cooperation with the **Western Balkans** partners, implementing the October 2018 Joint Action Plan on Counter-Terrorism for the Western Balkans. On 9 October, the Commission signed two non-binding bilateral counter-terrorism arrangements with Albania and the Republic of North Macedonia.[75] These arrangements set out tailor-made priority actions to be taken by the authorities of respective partner country, covering the five objectives of the Joint Action Plan[76] and indicating the support which the Commission envisages to provide. Similar arrangements with the remaining Western Balkans partners are expected to be signed in the coming weeks. Moreover, on 7 October 2019, the

---

73 COM(2019) 420 final (27.9.2019).

74 COM(2019) 416 final (13.9.2019).

75 https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en

76 The Joint Action Plan foresees actions around the following five objectives: a robust framework for countering terrorism; the effective prevention and countering of violent extremism; effective information exchange and operational cooperation; building capacity to fight money laundering and combat terrorism financing; strengthening the protection of citizens and infrastructure.

Commission signed an agreement with Montenegro on border management cooperation between Montenegro and the European Border and Coast Guard Agency (EBCGA). This agreement enables the Agency to assist Montenegro in border management with the aim to tackle irregular migration and cross-border crime, thus enhancing security at the EU's external border.

In order to enhance the cooperation with partner countries in tackling shared security threats, the Commission calls on the Council:

- to adopt the authorisation for the launch of negotiations for an agreement between the EU and **New Zealand** on the exchange of personal data to fight serious crime and terrorism;
- to adopt the authorisation for the launch of negotiations for an agreement between the EU and **Japan** on the transfer of passenger name record data;
- to adopt the proposed **Council Decision on the position to be taken on behalf of the EU in the International Civil Aviation Organization** with regard to standards and recommended practices on passenger name record data.

VI. CONCLUSION

This report sets out the wide range of measures that the EU has been taking to address common threats in Europe and enhance our collective security. Driven by a shared understanding that today's security challenges are best tackled by working together and with third countries, the progress made towards an effective and genuine Security Union is the result of close cooperation between a wide range of actors, building trust, sharing resources and facing threats together: across all levels of government, from cities and other local actors, regions and national authorities to the EU level with the European Parliament and the Council; involving public authorities, EU agencies, private actors and civil society; and using expertise, tools and resources across policy areas, such as transport policy, the digital single market or cohesion policy. In doing so, the work in the Security Union is embedded in the protection of fundamental rights, safeguarding and promoting our values.

The work towards an effective and genuine Security Union must continue. There is a need for swift agreement on important pending initiatives, notably: (1) the legislative proposal on the removal of terrorist content online, (2) the legislative proposal to improve law enforcement access to electronic evidence, (3) the legislative proposal setting up a European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres, and (4) the pending legislative proposals on stronger and smarter information systems for security, border and migration management. Agreed measures and instruments have to be turned into an operational reality on the ground, with timely and full implementation of EU legislation by all Member States to gain all its benefits for security. In particular, it is essential that all Member States implement the recently agreed legislation on the interoperability of EU information systems for security, border and migration management in order to attain the ambitious objective of achieving full interoperability by 2020. Finally, Europe needs to remain vigilant about emerging and changing threats, and keep working together to enhance the security of all citizens.