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

Seventeenth Progress Report towards an effective and genuine Security Union

I. INTRODUCTION

This is the seventeenth 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. The European Parliament and the Council made significant progress on a number of legislative priorities over the last months. However, for a large number of important priority files, political agreement is still pending and the co-legislators need to make further efforts. With the next European Parliament elections taking place in May 2019, time is of the essence in order to deliver on the pending priority proposals put forward by the Commission to complete the Security Union, as called for by President Jean-Claude Juncker in his 2018 State of the Union address.

At the European Council[1] meeting of 18 October 2018, EU leaders reaffirmed their commitment to strengthen the Union's internal security, acknowledging that real progress has been made in recent years to strengthen internal security through better cooperation, concrete measures on the ground, and the adoption of a range of legal texts. Building on that, the European Council called for progress on pending Commission proposals to prevent, respond to and deter cyber-attacks, prevent the dissemination of terrorist content online, ensure swift and efficient cross-border access to electronic evidence, facilitate access to financial information, and improve the interoperability of information systems and databases. This report provides the state of play of negotiations on these important initiatives, calling on the co-legislators to work towards their swift adoption (see also the list of all initiatives in the Security Union in Annex I). The European Council also called for examining the Commission's initiative to extend the competences of the European Public Prosecutor's Office to cross-border terrorist crimes, and for the Commission it is important to explore the benefits of this approach. Moreover, the Heads of State or Government emphasised the importance of protecting the Union's democratic systems and on combatting disinformation in the context of the upcoming European elections. The next European Council meeting on 13 and 14 December 2018 will also address the spread of disinformation campaigns as an acute challenge for democratic systems that requires urgent action, notably to ensure free and fair European and national elections. In light of that, this report takes account of progress made on ensuring electoral resilience within the Union.

In their Joint Declaration on the EU's legislative priorities for 2018-19[2] the Presidents of the European Parliament, the Council and the Commission identified the protection of the security of EU citizens to be amongst the highest priorities. The three institutions committed to treating proposals within the Security Union as urgent priority files to be adopted before the end of the current legislative term. Building on the progress already made over the last year, work needs to continue and the Commission urges the co-legislators to step up efforts in the negotiations.

The Commission looks forward to the adoption by the European Parliament of the report on findings and recommendations of the Special Committee on Terrorism that is planned for 12 December 2018. The report will be an important contribution to the work on countering terrorism and the further development of the Security Union.

---

[1] https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf
[2] https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-eu-legislative-priorities-2018-19_en.pdf

II. DELIVERING ON LEGISLATIVE PRIORITIES

The co-legislators have made significant progress on a number of legislative priorities over the last months, notably on a reinforced Schengen Information System, on the Cybersecurity Act and on non-cash means of payment. However, for a large number of important priority files, political agreement is still pending and further efforts are needed to ensure their adoption before the European Parliamentary elections (see also the list of all initiatives in the Security Union in Annex I).

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

The Commission welcomes the good progress made by the European Parliament and the Council on the legislative proposals to achieve **interoperability of EU information systems** for security, border and migration management.[3] The proposals would provide Member States' border guards, immigration officials and law enforcement officers with accurate and reliable information, and the ability to detect multiple identities and counter identity fraud. Trilogue meetings took place on 24 October 2018, 15 November 2018 and 27 November 2018. In line with the Joint Declaration, the Commission urges the co-legislators to reach political agreement at the next trilogue meeting on 13 December 2018.

The interoperability of information systems would include the **Visa Information System**. Work is ongoing in the European Parliament and in the Council on the May 2018 legislative proposal[4] to allow for more thorough background checks on visa applicants, close security information gaps through better information exchange between Member States and ensure full interoperability with other EU-wide databases. The Commission calls on the co-legislators to adopt their negotiating mandates as soon as possible, in order to reach agreement on this file during the current term of the European Parliament.

Once agreed, the interoperability of information systems would also allow exploiting the full benefits of the **reinforced Schengen Information System** as adopted by the co-legislators on 28 November 2018.[5]

Interoperability would also include the proposed[6] extension of the **European Criminal Records Information System** to third-country nationals. The proposal foresees establishing a centralised database that will make it possible to verify quickly if any Member State holds conviction information on a non-EU citizen. The Commission calls on the co-legislators to conclude the negotiations on this priority legislative initiative at the next trilogue meeting on 11 December 2018.

The interoperability of information systems would also include Eurodac. The Commission proposal to strengthen **Eurodac**[7] would expand its remit 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. The Commission has recently set out the benefits of adopting this proposal as one of five proposals under the Common European Asylum System

---

[3]   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).
[4]   COM(2018) 302 final (16.5.2018).
[5]   COM(2016) 881 final (21.12.2016), COM(2016) 882 final (21.12.2016), COM(2016) 883 final (21.12.2016).
[6]   COM(2017) 344 final (29.6.2017).
[7]   COM(2016) 272 final (4.5.2016).

close to agreement.[8] These proposals should be adopted before the European Parliamentary elections.

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

Joint Declaration priorities:
- to reach an agreement on the legislative proposals on **interoperability** by the end of this year;
- to reach an agreement on the legislative proposal to extend the **European Criminal Records Information System** to third-country nationals by December 2018;
- to adopt the legislative proposal on **Eurodac** on which agreement is within close reach, before the European Parliamentary elections.

Other:
- to adopt their respective negotiating mandates as soon as possible on the legislative proposal to strengthen the **Visa Information System**.

---

2. Strengthening security through enhanced external border management

Strong and reliable protection of the external borders is a precondition for security in the area of free movement without internal border controls. This is a shared task between 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 from June 2018[9], in September 2018 the Commission proposed[10] to further consolidate the European Border and Coast Guard to equip the Agency for more reliable and constant support capability. The Commission's proposal maintains the primary responsibility of Member States for the protection of the external borders, but will give the Agency the tools to back this up with a standing corps of 10 000 European border guards. Its gradual but swift establishment would provide an immediate boost to the EU's collective ability to protect the external borders and effectively carry out returns from the EU.

At the Justice and Home Affairs Council on 6 December 2018, a partial general approach was reached on the return and external related aspects of the Commission's proposal. However, work will need to be intensified on all aspects of the proposal with a view to obtain a mandate as soon as possible in January to start the trilogues with the European Parliament. In the European Parliament, the report of the Committee on Civil Liberties, Justice and Home Affairs is expected to be adopted in January 2019. This proposal is a clear priority for the European Union, and the Commission calls on the European Parliament and the Council to adopt the proposed legislation during the current term of the European Parliament.

To strengthen security through enhanced external border management, the Commission calls

---

8   Managing Migration in all its Aspects: Progress on the European Agenda on Migration, COM(2018) 798 final (4.12.12).
9   https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf
10   COM(2018) 631 final (12.9.2018).

on the European Parliament and the Council:

2018 State of the Union initiatives:
- to adopt as soon as possible their full negotiating mandates on the legislative proposal to strengthen the **European Border and Coast Guard**, in order to adopt the legislation during the current term of the European Parliament.

3. Preventing radicalisation

Negotiations are well underway in the Council on the proposal for Regulation on **Terrorist Content Online** as proposed by the Commission together with the 2018 State of the Union.[11] Its purpose is to provide a clear, harmonised legal framework to prevent the misuse of hosting service providers for the dissemination of terrorist content, whilst ensuring the full protection of fundamental rights. The proposed Regulation responds to urgent calls from both the European Council[12] and the European Parliament.[13] The Commission welcomes the adoption of a general approach at the Justice and Home Affairs Council on 6 December 2018. The Commission urges the European Parliament to speed up its work on this proposal, with a view to its adoption under the current legislature.

In parallel, the Commission remains fully committed to supporting Member States and hosting service providers in their efforts to tackle terrorist content online. The **EU Internet Forum** will continue to promote Member States' and hosting service providers' voluntary cooperation and actions to reduce the accessibility to terrorist content online, and to empower civil society to increase the volume of effective, alternative narratives online. The fourth Ministerial EU Internet Forum took place on 5 December 2018. It took stock of progress over the last twelve months in removing terrorist content from the internet.

The Commission also continues to **support the prevention of radicalisation in Member States**. In its inaugural meeting in Vienna on 24 October 2018, the Steering Board for Union actions on preventing and countering radicalisation[14] agreed the annual strategic orientations for actions and initiatives at EU level for 2019. The strategic priorities build on insights from practitioners (conclusions from the Radicalisation Awareness Network High-Level Conference and the Radicalisation Awareness Network Plenary of 11 and 12 October 2018), researchers (the Radicalisation Awareness Network Research Conference of 17 October 2018), other EU networks and initiatives (such as in particular the European Strategic Communications Network) as well as contributions from policy makers.

As part of the 2018 work programme of the **Internal Security Fund** for police cooperation and crime prevention, on 28 November 2018 the Commission launched a call for proposals for targeted funding of EUR 5 million for preventing and countering radicalisation addressing

---

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

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

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

[14] C(2018) 5345 (9.8.2018).

priority areas identified by the High-Level Commission Expert Group on Radicalisation: community engagement, local dimension, multi-agency approach and youth.[15] In addition, civil society organisations seeking to counter terrorist narratives by providing positive alternatives will be supported with EU funding through the Civil Society Empowerment programme, which has earmarked EUR 12 million in training and funding civil society partners to mount counter-terrorist narrative campaigns online.

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

2018 State of the Union initiative:
- to adopt as a matter of priority its negotiating mandate on the legislative proposal to prevent the dissemination of **terrorist content online**, in order to adopt the legislation during the current term of the European Parliament.

---

4. *Addressing disinformation and ensuring electoral resilience*

As called for by the European Council in June 2018, the Commission and the High Representative, in cooperation with the Member States, presented on 5 December 2018 an **Action Plan**[16] with further specific proposals for a coordinated EU response to the **challenge of disinformation**, including appropriate mandates and increased resources for the relevant Strategic Communication teams of the European External Action Service.

Moreover, the Commission is closely monitoring the implementation of the actions to counter disinformation announced in its April 2018 Communication on Tackling online disinformation.[17] On 16 October 2018, initial signatories subscribed to the **Code of Practice on Disinformation** for online platforms and the online advertising sector. These include the three major platforms (Facebook, Google/YouTube, Twitter) and the internet browser provider Mozilla, plus trade associations representing other online platforms and the advertising sector. The Code includes 15 commitments centred around five chapters: (1) scrutiny of advertisement placements; (2) political advertising and issue-based advertising; (3) integrity of services; (4) empowering consumers; and (5) empowering the research community. The Commission will conduct a close and continuous monitoring of the Code's implementation in its first 12 months, in particular in view of the 2019 European Parliament elections.[18] Should the implementation and the impact of the Code of Practice prove to be unsatisfactory, the Commission may propose further measures, including of a regulatory nature.

In order to help ensure **electoral resilience**, the Commission has tabled a number of initiatives to address the threat of attacks against electoral infrastructure and campaign information systems and the risk of misuse of personal data in order to deliberately influence the outcome of the European elections. On 12 September 2018, the Commission adopted a

---

[15] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/isfp-2018-ag-ct-rad;freeTextSearchKeyword=;typeCodes=1;statusCodes=31094501,31094502;programCode=ISFP;programDivisionCode=null;focusAreaCode=null;crossCuttingPriorityCode=null;callCode=Default;sortQuery=openingDate;orderBy=asc;onlyTenders=false

[16] JOIN (2018) 36 (5.12.2018).

[17] COM(2018) 236 final (26.4.2018).

[18] COM(2018) 794 (5.12.2018).

Communication on securing free and fair elections[19] and a Recommendation on election cooperation networks, online transparency protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament. The European elections cooperation network will provide a forum for the coordination of the implementation of the Recommendation, and Council Conclusions on these measures are planned for early 2019.

Together with the Communication and the Recommendation, the Commission also put forward guidance on the application of EU data protection law, aimed to assist relevant actors in the application of the data protection obligations under EU law in the electoral context[20], as well as a **legislative proposal for a targeted change of the 2014 Regulation on party funding**.[21] The European Parliament Committee on Constitutional Affairs voted on its report on 6 December 2018 and the European Parliament's plenary is due to adopt its negotiating mandate in the December 2018 session. The Commission calls on the Council to adopt its negotiating mandate in December 2018 so that both co-legislators can start with trilogue sessions without delay, so as to ensure that the proposed targeted changes are in place in time for the 2019 to the European Parliament elections.

On 15 and 16 October, the Commission organised a **High-Level Conference on cyber-threats to elections**, aiming at informing the European Commission's ongoing work towards improving the security and resilience of electoral processes against constantly evolving cyber-enabled threats. The event gathered leading experts from around the world to discuss how best to follow up on existing initiatives. The conference was followed by a High-Level Member States' Workshop organised with the aim to bring together national electoral commissions and cybersecurity officials. This was the first occasion on which electoral and cybersecurity authorities met together to discuss how best to address cyber-threats to elections.

The **Colloquium on Fundamental Rights** on 26-27 November 2018 brought together high-level national and European policymakers, academics and representatives from civil society, the media, international organisations and the private sector to debate the broad subject of democracy in the EU. The Colloquium's conclusions will inform the work of the European elections cooperation network, which the Commission will bring together for the first time in January.

To address disinformation and ensure electoral resilience, the Commission calls on the European Parliament and the Council:

2018 State of the Union initiatives:
- to ensure that the proposed **targeted changes of the Regulation on party funding** are in place in good time for the 2019 elections to the European Parliament.

Letter of Intent 2018:
- to implement swiftly and decisively the actions of the **Joint Action Plan against Disinformation** as presented by the European Commission on 5 December 2018.

---

5. *Enhancing cybersecurity*

---

[19] COM(2018) 637 final (12.9.2018).
[20] COM(2018) 638 final (12.9.2018).
[21] COM(2018) 636 final (12.9.2018).

As part of the actions set out in the September 2017 Joint Communication[22] on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", the co-legislators held five trilogue meetings from 13 September 2018 to 10 December 2018 on the proposed **Cybersecurity Act**[23] and have reached political agreement. The Act, which will now be formally adopted and come into force as soon as possible, strengthens the mandate of the EU Agency for Network and Information Security. It also establishes an EU cybersecurity certification framework for information and communications technology products, services and processes.

The Commission welcomes the progress made on its legislative proposal on **non-cash means of payment**.[24] The proposed rules will update the EU's legal framework against fraud and counterfeiting of non-cash means of payment, addressing new challenges and technological developments such as virtual currencies and mobile payments, removing obstacles to operational cooperation and enhancing prevention measures and assistance for victims. Trilogues discussions started in September 2018, with the most recent one held on 28 November 2018 leading to a provisional agreement. The Commission calls on the co-legislators to conclude the negotiations on this file at the next trilogue meeting on 12 December 2018.

Building on the ambitious cybersecurity initiatives announced in 2017, the September 2018 Commission proposal for a Regulation setting up a **European Cybersecurity Industrial, Technology and Research Competence Centre**, **with a Network of National Coordination Centres**, aims to support cybersecurity technological and industrial capacities and is a cornerstone for a Europe that protects. This goes hand-in-hand with the key objective to increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into competitive advantage of other European industries. The Commission calls on the European Parliament and the Council to adopt their respective negotiating mandates swiftly with a view to entering trilogue discussions as soon as possible, taking into account the ongoing negotiations on the Digital Europe programme.

Given the global nature of cyber threats, international cooperation on cybersecurity is essential. On 23-24 October 2018, representatives from the US Department of Homeland Security and the European Commission met for a **workshop on cybersecurity policy approaches** in order to explore avenues for increased collaboration. Participants identified several opportunities to facilitate bilateral engagement and encouraged further working level exchanges on respective certification of information, supply chain risk management, workforce and skill management as well as research and development priorities with regards to cybersecurity.

Over the last months, the European External Action Service, in cooperation with the Commission, held another round of **Cyber Dialogues** with the United States (10 September 2018), China (16 November 2018) and is planning one with India on 12 December 2018. The dialogues addressed the implementation of cyber norms, cyber security confidence building measures and the application of international law in cyberspace. Significant progress has also been achieved in the last months in the implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the "**cyber diplomacy toolbox**")[25], as

---

22	JOIN(2017) 450 final (13.9.2017).
23	COM(2017) 477 final (13.9.2017).
24	COM(2017) 489 final (13.9.2017).
25	Council document 9916/17.

called by the European Council in June 2018 and in its October 2018 conclusions on setting up the EU restrictive measures on cyber attacks.

To enhance cybersecurity, the Commission calls on the European Parliament and the Council:

2018 State of the Union initiatives:
- to adopt as soon as possible their negotiating mandate on the legislative proposal on the **European Industrial, Technology and Research Cybersecurity Competence Centre** and the **Network of National Coordination Centres**, in order to advance as much as possible during the current term of the European Parliament.

Other:
- to finalise agreement in December 2018 on the legislative proposal on **non-cash means of payment**.

---

6. *Closing down the space in which terrorists operate*

Effective investigation, prosecution and sentencing of crime relies heavily on electronic evidence. The availability of such evidence is of particular importance in the prosecution of cross-border crimes such as terrorism or cybercrime. The Commission welcomes the adoption by the Justice and Home Affairs Council on 7 December 2018 of a general approach on the April 2018 Commission proposed Regulation to improve the cross-border access to **electronic evidence** in criminal investigations.[26] Given the importance of electronic evidence for criminal investigations in almost all types of crime and considering the Joint Declaration, the Commission urges the European Parliament to speed up its work on this proposal with a view to its adoption under the current legislature.

With regard to **international developments on electronic evidence**, the Commission is closely following developments on the ongoing negotiations of a Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime on access to electronic evidence. In addition, an agreement with the United States would provide legal clarity for law enforcement authorities from both sides and avoid conflicting legal obligations for service providers. At the EU-US Justice and Home Affairs Ministerial Meeting in Washington on 8-9 November 2018, both the EU and the US representatives underlined the importance, for both law enforcement and judicial authorities, of swift cross-border access to electronic evidence. It is the Commission's intention to propose, jointly and as soon as possible, the adoption of two recommendations for negotiating directives on these two international aspects, taking into account the progress made in the discussions on the electronic evidence proposals and the need for sufficient clarity about the parameters and safeguards of the future EU internal arrangements.

Given the importance to allow access by law enforcement to financial information, the Commission adopted, in April 2018, a legislative proposal to **facilitate the use of financial and other information** for the prevention, detection, investigation or prosecution of serious criminal offences.[27] The proposal seeks to provide designated law enforcement authorities and

---

[26] COM(2018) 225 final (17.4.2018). Negotiations on the accompanying Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (COM(2018) 226 final (17.4.2018)) will continue.

[27] COM(2018) 213 final (17.4.2018).

Asset Recovery Offices with direct access to bank account information held in national centralised bank account registries, and to strengthen cooperation between national Financial Intelligence Units and law enforcement authorities. On 21 November 2018, the Council adopted a general approach on the file. Following the adoption of the report by the Committee on Civil Liberties, Justice and Home Affairs on 3 December 2018, the European Parliament is expected to agree its negotiation mandate during the December 2018 plenary session. The Commission welcomes the progress made and urges the co-legislators to move forward with the inter-institutional negotiations without delay to reach an agreement before the European elections.

In April 2018, the Commission tabled a legislative proposal on **restrictions on the marketing and use of explosives precursors**[28] to restrict access to dangerous explosives precursors that might be misused to make homemade explosives. The proposal seeks to close security gaps with a number of 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. The European Parliament Committee on Civil Liberties, Justice and Home Affairs is expected to adopt its report on 10 December 2018. Given the progress achieved on this file, the Commission calls on the Council to adopt its negotiating mandate still in December 2018, and on both co-legislators to agree during the current term of the European Parliament.

Another legislative proposal tabled by the Commission in April 2018 aimed to strength the security of identity cards of Union citizens and of residence documents.[29] The proposal notably introduces minimum **security features for identity cards**, which will need to include biometric identifiers (a facial image and two fingerprints) on a contactless chip. The proposal is listed as a priority pending proposal under the Commission Work Programme for 2019. On 14 November 2018, the Council adopted a mandate to enter into negotiations with the Parliament on the proposal. On 3 December 2018, the Parliament agreed to enter negotiations on the basis of the report of the Committee on Civil Liberties, Justice and Home Affairs. Trilogue discussions will start imminently and the Commission is committed to support the co-legislators for an adoption of the proposal before the next European Parliament elections which is now within reach.

---

[28]   COM(2018) 209 final (17.4.2018).
[29]   COM(2018) 212 final (17.4.2018).

To close down the space in which terrorists operate, the Commission calls on:

Joint Declaration priorities:
- the European Parliament to adopt as a matter of urgency its negotiating mandate on the legislative proposals on **electronic evidence** and enter into trilogue discussions with the Council without delay;
- the European Parliament and the Council to find an agreement on the legislative proposal to **facilitate the use of financial data** before the European Parliament elections.

Other:
- the European Parliament and the Council to adopt their negotiating mandate by the end of 2018 on the legislative proposal to strengthen the **restrictions on the marketing and use of explosives precursors**;
- the European Parliament and the Council to find an agreement on the legislative proposal to enhance the **security features of national identity cards and residence documents** for it to be adopted before the European Parliamentary elections.

III. IMPLEMENTATION OF OTHER PRIORITY FILES ON SECURITY

1. Implementation of legislative measures in the Security Union

To ensure benefits of an effective and genuine Security Union, the full and correct implementation of agreed measures is a paramount priority. 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 the deadline for the implementation of the **EU Passenger Name Record Directive**[30] passed on 25 May 2018, the Commission launched infringement procedures on 19 July 2018 against 14 Member States for failing to communicate the adoption of national legislation which fully transposes the Directive[31] – a critical tool in the fight against terrorism and serious crime. Since then, five Member States have notified full transposition.[32] 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**[33] expired on 8 September 2018. The Commission launched infringement procedures on 21 November 2018

---

[30] Directive (EU) 2016/681 (27.4.2016).
[31] Bulgaria, Czech Republic, Estonia, Greece, Spain, France, Cyprus, Luxembourg, Netherlands, Austria, Portugal, Romania, Slovenia and Finland. The Commission is receiving replies by Member States, including notifications of the legislation concerned, which are currently being analysed (see also footnote 47).
[32] Bulgaria, France, Luxembourg, Austria and Greece (state of play as of 6 December 2018).
[33] Directive (EU) 2017/541 (15.3.2017).

against 16 Member States for failing to communicate the adoption of national legislation which fully transposes the Directive.[34]

The deadline for transposition of the **Directive on the control of the acquisition and possession of weapons**[35] expired on 14 September 2018. The Commission therefore launched infringement procedures on 22 November 2018 against 25 Member States for failing to communicate the adoption of national legislation which fully transposes the Directive.[36] Following the launch of infringement procedures, one more Member State notified full transposition of measures.[37]

The deadline for transposing the **Data Protection Law Enforcement Directive**[38] into national law expired on 6 May 2018. The Commission launched infringement procedures on 19 July 2018 against 19 Member States for failing to communicate the adoption of national legislation which fully transposes the Directive.[39]

According to what Member States notified to the Commission, the **Directive on the security of network and information systems**[40] has been fully transposed in 21 Member States and partially transposed in other 3 Member States.[41] The Commission has carried out *prima facie* checks for 18 out of 21 Member States, which confirmed that transposition seems complete. On 19 July 2018, the Commission had launched infringements for lack of full notification against those 17 Member States that had not notified within the transposition deadline of 9 May 2018.[42]

By 9 November 2018, Member States had to submit to the Commission information about the so-called operators of Essential Services identified within their territory, as part of the transposition of the Directive on the security of network and information systems. These are public and private entities that, pursuant to the Directive's requirements, should secure their network and information systems and report serious incidents. So far, 19 Member States shared feedback with the Commission and 16 submitted the relevant information to the

---

[34]   Belgium, Bulgaria, Czech Republic, Estonia, Greece, Spain, Croatia, Cyprus, Lithuania, Luxembourg, Malta, Austria, Poland, Portugal, Romania and Slovenia.

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

[36]   Belgium, Bulgaria, Czech Republic, Germany, Estonia, Ireland, Greece, Spain, France, Cyprus, Latvia, Lithuania, Luxembourg, Hungary, Malta, Netherlands, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Finland, Sweden, United Kingdom.

[37]   France (state of play as of 6 December 2018).

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

[39]   Belgium, Bulgaria, Czech Republic, Estonia, Greece, Spain, France, Croatia, Cyprus, Latvia, Lithuania, Luxembourg, Hungary, Netherlands, Poland, Portugal, Romania, Slovenia and Finland. The Commission is receiving replies by Member States, including notifications of the legislation concerned, which are currently being analysed (see also footnote 51).

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

[41]   Bulgaria, Czech Republic, Denmark, Germany, Greece, Estonia, Ireland, Spain, France, Croatia, Italy, Cyprus, Malta, Netherlands, Poland, Portugal, Slovenia, Slovakia, Finland, Sweden and the United Kingdom notified full transposition. Lithuania, Hungary and Latvia notified partial transposition (state of play as of 6 December 2018).

[42]   Belgium, Bulgaria, Denmark, Ireland, Greece, Spain, France, Croatia, Latvia, Lithuania, Luxembourg, Hungary, Netherlands, Austria, Poland, Portugal and Romania. The Commission is receiving replies by Member States, including notifications of the legislation concerned, which are currently being analysed (see also footnote 48).

Commission.[43] The Commission will now assess the input received with a view to compiling a report on the consistency of the approach taken by Member States in the identification process.

The Commission is also assessing the transposition of the **4th Anti-Money Laundering Directive**[44] and is working to ensure that the rules are implemented on the ground. The Commission has launched infringement procedures against 21 Member States for failing to communicate the adoption of national legislation transposing the Directive.[45] It will continue to use its powers when appropriate to ensure full implementation of this Directive. Complementing this Directive, on 3 December 2018, new criminal law measures to counter money laundering entered into force in the EU. The new Directive[46] will harmonise offences and sanctions for money laundering by providing for equally severe penalties across the EU, with a minimum term of imprisonment of 4 years. Member States have 24 months to transpose this Directive and to notify the Commission accordingly.

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

Since the transposition deadlines have expired, the Commission has launched the infringement procedures and calls on Member States, as a matter of urgency, to take the necessary measures to fully transpose the following directives into national law and communicate this to the Commission:

- the **EU Passenger Name Record Directive**, where 6 Member States still need to notify transposition into national law and 3 Member States need to complete the notification of transposition;[47]
- the **Directive on security of network information systems**, where 4 Member States still need to notify transposition into national law and 3 Member States need to complete the notification of transposition;[48]
- the **Directive on combating terrorism**, where 7 Member States still need to notify transposition into national law and 9 Member States need to complete the notification of transposition;[49]
- the **Directive on the control of the acquisition and possession of weapons**, where

---

[43] Cyprus, Czech Republic, Germany, Denmark, Estonia, Spain, Finland, France, Croatia, Hungary, Lithuania, Netherlands, Poland, Portugal, Sweden and the United Kingdom (state of play as of 6 December 2018).

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

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

[46] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law.

[47] Spain, Cyprus, Netherlands, Portugal, Romania and Finland are yet to communicate transposition. Czech Republic, Estonia and Slovenia communicated partial transposition and are yet to complete the notification of transposition (state of play as of 6 December 2018).

[48] Belgium, Luxembourg, Austria and Romania are yet to communicate transposition. Lithuania, Hungary and Latvia communicated partial transposition and are yet to complete the notification of transposition (state of play as of 6 December 2018).

[49] Bulgaria, Greece, Cyprus, Luxembourg, Malta, Poland and Romania are yet to communicate transposition. Belgium, Czech Republic, Estonia, Spain, Croatia, Lithuania, Austria, Portugal and Slovenia communicated partial transposition and are yet to complete the notification of transposition (state of play as of 6 December 2018).

> 19 Member States still need to notify transposition into national law and 5 need to complete the notification of transposition;[50]
> - the **Data Protection Law Enforcement Directive**, where 11 Member States still need to notify transposition into national law and 2 Member States need to complete the notification of transposition;[51] and
> - the **4ᵗʰ Anti-Money Laundering Directive**, where 3 Member States need to complete the notification of transposition.[52]

2. Preparedness and protection

One year after the adoption of the 2017 Commission Action Plan on the **protection of public spaces**[53], significant progress has been made in its implementation across all areas, with a particular focus on providing guidance and EU funding to support Member States.

Six meetings with public authorities and private operators took place to share good practices and exchange information on how operators and public authorities can strengthen the security of different types of public spaces, including hotels, shopping centres, transport venues, sports stadia and cultural venues. While both public authorities and operators are taking initiatives to strengthen the security of their venues, the meetings have shown that there are remaining challenges and gaps. While some sectors have a well-developed security culture, others are only now putting in place more systematic approaches to protecting their venues. The Operators Forum, a Commission-led group to encourage public-private security partnerships, held a meeting involving all sectors on 26 November 2018. The participants welcomed the guidance provided by the Commission services setting out good practices for measures that operators and public authorities should implement to strengthen the security of public spaces.

Following the Commission's technical workshop with urban planners and local security officials from European cities held in June 2018, the Commission's Joint Research Centre prepared two reports mapping existing guidance material for public space protection and barrier systems. A first European guideline on the selection of proper barrier solutions has also been drafted enabling urban planners to enhance urban security without creating fortress-like city centres.

EU funding also supports this work. Under the Internal Security Fund-Police 2017 protect call, eight projects which focus on the protection of public spaces were selected, ranging from urban security concepts, enhancing security by design, protection against vehicle ramming attacks, improving the protection level in rail security and developing training concepts as well as campaigns to raise awareness. Further actions will be funded under the 2018 call for

---

[50] Belgium, Bulgaria, Germany, Estonia, Ireland, Greece, Spain, Cyprus, Latvia, Luxembourg, Hungary, Netherlands, Austria, Poland, Romania, Slovenia, Slovakia, Finland and Sweden are yet to communicate transposition. Czech Republic, Lithuania, Malta, Portugal and the United Kingdom communicated partial transposition and are yet to complete the notification of transposition (state of play as of 6 December 2018).

[51] Bulgaria, Estonia, Greece, Spain, Cyprus, Latvia, Netherlands, Poland, Romania, Slovenia and Finland are yet to communicate transposition. Czech Republic and Portugal communicated partial transposition and are yet to complete the notification of transposition (state of play as of 6 December 2018).

[52] Luxembourg, Austria and Romania communicated partial transposition and are yet to complete the notification of transposition. The remaining 18 Member States have notified full transposition and the assessment by the Commission is ongoing (state of play as of 6 December 2018).

[53] COM(2017) 612 final (18.10.2017).

proposals under the Internal Security Fund-Police.[54] A call for proposals under the Urban Innovative Actions initiative as part of the European Regional Development Fund[55] is also open, intending to provide cities with innovative solutions to address urban security challenges. Moreover, a dedicated research call has been included in the Horizon 2020 Secure Societies work programme 2018-2020 with the aim of developing innovative solutions for the protection of public spaces.

As requested by the European Council at its March 2018 and October 2018 meetings, the Commission has stepped up its **actions against Chemical, Biological, Radiological and Nuclear threats** and its collaboration with Member States in particular on chemical threats. Commission and Member States experts have developed a common list of chemical substances of concern and will work now with manufacturers on the improvement of the detection capabilities. The Commission also launched a dialogue with the private sector to explore possibilities of reducing accessibility of terrorists to chemical substances which can be used as precursors for chemical attacks. The Commission is also conducting a training campaign in its dedicated European Nuclear Security Training Centre in order to train national law enforcement authorities on detection of radiological and nuclear materials. More than 100 police officers will train using sophisticated equipment and actual nuclear material in order to be better prepared for a potential dirty bomb attack.

As a follow-up to the conclusions of the June 2018 European Council, the Foreign Affairs Council adopted on 15 October 2018 a **new regime of restrictive measures** to address the use and proliferation of chemical weapons. It will enable the EU to impose sanctions, consisting of travel bans to the EU and asset freezing for persons and entities involved in the development and use of chemical weapons anywhere, regardless of their nationality or location.[56]

From 5 November to 23 November 2018, the EU and NATO carried out the **EU-NATO Hybrid Exercise** as a parallel and coordinated exercise. The aim was to improve and enhance, in a safe-to-fail environment, the EU's ability to respond to a complex crisis of a hybrid nature with an internal and an external dimension, as well as to improve cooperation with NATO. The exercise involved relevant EU institutions and bodies, with the participation of 25 Member States plus Norway and eight EU Agencies. Switzerland acted as observer.

With regards to **preparedness and protection**, the Commission:

- calls on Member States to work towards the full implementation of the Action Plan to enhance preparedness against Chemical, Biological, Radiological and Nuclear risks by the end of 2019;
- calls on Member States and the private sector to step up cooperation to improve the protection of public spaces and to work towards full implementation of the Action Plan on the Protection of Public Spaces.

---

[54] https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police/union-actions_en, call open until 16 January 2019.
[55] https://www.uia-initiative.eu/en/urban-security, call open until 31 January 2019.
[56] Council Regulation (EU) 2018/1542 of 15 October 2018 concerning restrictive measures against the proliferation and use of chemical weapons.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1542

3. Security research

EU security research is one of the building blocks of the Security Union enabling innovation in technologies and knowledge crucial for developing capabilities to address today's security challenges, anticipating tomorrow's threats and contributing to a more competitive European security industry. This is especially important given the need to consider strategic security issues such as the digital infrastructure supply chain and the provenance of technological components.

Compared to other fields, EU funding is of crucial importance to security research representing around 50% of all public funding for security research at EU and national level.[57] Since the inception of security research at EU level in 2007, the EU has contributed more than EUR 2 billion in funding to over 400 projects, including in areas subject to EU policy developments such as airport scanners, advanced forensics, tools to deal with online radicalisation, methods for gathering electronic evidence in criminal cases, and technologies for first responders. Future technological trends such as Artificial Intelligence, cognitive systems and data analytics are also well represented in ongoing projects.

Recent projects have demonstrated the direct link between research and the implementation and development of policy: in border security and supply chain management[58], in Chemical, Biological, Radiological and Nuclear risks[59], in the handling of electronic evidence[60], and in the area of maritime surveillance[61].

Given the particular nature of the security sector (in which the market is represented mainly by public authorities), appropriate uptake of research output can be guaranteed only if research is acknowledged as one of the building blocks of a wider capability development process bringing together policy-makers, practitioners, industry and academia. The close involvement of all stakeholders at an early stage is instrumental to identify capability gaps, and define capability priorities that can, when needed, trigger research requirements. The Commission is working in close collaboration with all relevant stakeholders to promote such an approach.

---

[57]   Only eight Member States have declared having in place a structured national security research programme.

[58]   The CORE project pioneered the use of block chain technology in supply chain management. Several major logistic companies, e.g. MAERSK-IBM, Seacon Logistics, and Royal Flora Holland are taking forward the developments in CORE in building their internet-based logistics systems, Project ID 603993, FP7-SEC-2013-1, start 1.5.2014, details available at: https://cordis.europa.eu/project/rcn/188515_en.html

[59]   The TOXITRIAGE project provided a readily used detection system for chemical and biological threats and an efficient coordination mechanism for the triage of victims involving different types of first responders, Project ID 653409, H2020-DRS-2014, start 1.9.2015, details available at: https://cordis.europa.eu/project/rcn/194860_en.html

[60]   The EVIDENCE project defined a roadmap outlining strategies, objectives and actions needed to set up a Common European Framework for the correct and harmonised handling of electronic evidence. These results were used as input to the Inception impact assessment for the Commission legislative proposal in this area, Project ID 608185, FP7-SEC-2013-1, start 1.3.2014, details available at: https://cordis.europa.eu/project/rcn/185514_en.html

[61]   The Project CLOSEYE was the first example of how EU funded research could bridge the gap between the identification of a capability gap and the deployment of technology solutions to fill such gap. Building on previous EU funded research on maritime border surveillance, this project has led to solutions to improve the detection, identification and tracking of small boats at sea. As a result, two Member States authorities from Spain and Portugal have launched a procurement initiative based on the CLOSEYE outcome. Spain has used the ISF Borders instrument therefore fully exploiting the synergies between these different EU funds. Project ID 313184, FP7-SEC-2012-1, start 1.4.2013, details available at: https://cordis.europa.eu/project/rcn/108227_en.html

To raise awareness of the results, on 5-6 December, the **2018 Security Research Event** brought together in Brussels around 900 stakeholders from across Europe to demonstrate the impact of EU-funded security research. The same week also saw a gathering of the 'Community of Users on Secure, Safe and Resilient Societies' with dedicated panels around a series of security research topics, as well as the annual meeting of the International Forum to Advance Innovation for First Responders.

As part of its proposal for the future Research and Innovation Framework Programme (Horizon Europe**,** part of the next Multiannual Financial Framework which runs from 2021-2027), the Commission made clear that security research should continue to be an important priority. The Horizon Europe Programme will aim to achieve greater complementarities with other research programmes in areas such as defence, as well as synergies with related funding programmes such as the Internal Security Fund, the Integrated Border Management Fund including the Border Management and Visa Instrument, and the Digital Europe and Regional funds. The programme will also be targeted at further enhancing the role of the EU agencies and practitioners in the entire research cycle.

On 7 December 2018, the Commission adopted a Communication and a Coordinated Action Plan[62] on working together for **Artificial Intelligence** which covers the need to maximise the benefits of Artificial Intelligence in the security sector including law enforcement agencies and business. With the Coordinated Action Plan the Commission intends to transform principles into concrete actions to be implemented jointly by the Commission and Member States. All three security aspects of Artificial Intelligence[63] are prominently present in all actions from research until the placing of such technologies on the market.

The Commission is committed to embed the discussion about the risks and opportunities associated to Artificial Intelligence in a wider development strategy for security, taking into account various scenarios, needs, gaps and alternatives that are specific to each area of security. In addition, the Commission intends to discuss with the Secure Societies Programme Committee the inclusion of a relevant action already in the Horizon 2020 Work Programme for 2020.

With regards to **Security Research**, the Commission will:

- between March 2019 and August 2019, launch the Horizon 2020 Secure Societies calls for proposals for 2019.

---

4. External dimension

The EU had a valuable exchange with counterparts in the United States at the **EU-US Ministerial Meeting on Justice and Home Affairs** on 8 and 9 November 2018 in Washington, reaffirming their commitment jointly to address common challenges in the areas of justice and home affairs. In particular, there was a shared emphasis on the importance of effective information sharing in their efforts to combat terrorism. The EU and the US emphasised the importance of Passenger Name Records information sharing as a tool for the

---

[62]   COM(2018) 795 final (7.12.2018).
[63]   Cybersecurity of Artificial Intelligence based technologies, the exploitation of Artificial Intelligence for security purposes, including the prevention, detection and investigation of criminal offences and terrorism as well as the prevention of malicious and criminal use of Artificial Intelligence.

prevention of terrorist travel and agreed to prepare for a joint evaluation in 2019 in compliance with the provisions of the EU-US Passenger Name Record Agreement. Additionally, the EU and the US reiterated the priority they attach to fighting cybercrime and enhancing cybersecurity. Both sides agreed to explore the possibility of an EU-US Agreement on electronic evidence. The European Union and the United States also recognised the need to enhance their efforts to address the challenge of terrorists' use of the internet to direct and inspire attacks, while respecting individual rights, including the freedom of speech. Both sides recognised that electoral systems in democratic states face unprecedented challenges that require cooperation and best-practice exchanges between like-minded countries. The European Union and the United States agreed to set up a regular dialogue on these matters, starting at the next Senior Officials meeting in 2019.[64]

The negotiations between the EU and Canada on a **revised Passenger Name Record Agreement** continued. The Commission will continue to regularly debrief the Council and the European Parliament's Committee on Civil Liberties, Justice and Home Affairs on progress made.

On 30 November 2018, the first round of negotiations took place for an agreement between the EU and Turkey on the exchange of personal data between Europol and the Turkish authorities competent for fighting serious crime and terrorism. The Commission is also in contact with the Israeli authorities in view of a first round of negotiations with Israel. On 3 December 2018, a meeting was held between the EU and representatives from Algeria, Egypt, Jordan, Lebanon, Morocco and Tunisia to discuss possible future cooperation between law enforcement authorities in those countries and Europol, including via working arrangements and with a view to possible agreements to allow for the exchange of personal data.

The EU has continued to pursue **dialogues on counter terrorism** with partner countries. On 12 November 2018, the EU-India Counter Terrorism Dialogue in Brussels addressed information exchange, terrorist use of the internet, and possible cooperation with Europol. On 29 November 2018, the EU-Pakistan Counter Terrorism Dialogue in Brussels addressed efforts to combat terrorist financing in the context of the Financial Action Task Force. The EU-Algeria Dialogue on Counter-Terrorism and Regional Security on 12 November 2018 in Algiers led by High Representative/Vice-President Mogherini addressed efforts to restore security in Libya and the Sahel. A first EU-Kuwait Senior Officials meeting took place in Brussels on 27 November 2018 to discuss opportunities for further exchanges and potential future cooperation on issues related to counterterrorism, organised crime and cyber-security.

In November 2018, for the first time, Iraqi military and law enforcement actors have attended training in the collection of battlefield evidence at the NATO Stability Policing Centre of Excellence, in Vicenza, Italy at an Italian Carabinieri training-hub. This training is part of a three-year EU-INTERPOL-NATO project, which aims to ensure that individuals linked to serious crimes and terrorism in conflict zones are brought to justice. This project is a concrete EU action related to capacity building on the lawful collections of evidence of crimes committed by Da'esh militants, which could eventually lead to enhance the international cooperation between Iraqi and EU law enforcement agencies.

IV. CONCLUSION

The report shows the good progress that has been made in the work towards building an

---

[64] https://www.consilium.europa.eu/en/press/press-releases/2018/11/09/joint-eu-u-s-statement-following-the-eu-u-s-justice-and-home-affairs-ministerial-meeting/#

effective and genuine Security Union. However, it underlines at the same time that more effort is still required by the co-legislators and Member States in concluding legislative processes and implementing adopted measures in order to provide EU citizens with strengthened internal security. In view of the European elections in May 2019, the coming weeks will be decisive for making further progress on developing and putting in place appropriate security policies at EU level.