EUROPEAN
COMMISSION

Brussels, 13.6.2018
COM(2018) 470 final

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

Fifteenth Progress Report towards an effective and genuine Security Union

I. INTRODUCTION

This is the fifteenth report on the 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.

In the wake of the Salisbury nerve agent attack, the European Council[1] stated in March 2018 that "the EU must strengthen its **resilience to Chemical, Biological, Radiological and Nuclear-related risks** ("CBRN risks"), including through closer cooperation between the European Union and its Member States as well as NATO". It invited the Commission and the High Representative to take this work forward and report on progress by the June 2018 European Council. This Progress Report is part of the response to this call, together with a Joint Communication[2] on Increasing resilience and bolstering capabilities to address hybrid threats and a Joint Report[3] on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018. It takes stock and presents next steps in implementing the October 2017 Action Plan[4] to enhance preparedness against chemical, biological, radiological and nuclear security risks. As part of the measures in the Security Union to improve protection and resilience against terrorism, the Action Plan followed a preventive approach based on the rationale that threats posed by chemical, biological, radiological and nuclear substances were risks with low probability but high and lasting impact in case of an attack. In the meantime, the attack in Salisbury, as well as an increasing concern about terrorist interest and a capability to use such substances both inside and outside the EU[5], show that the threat posed by chemical, biological, radiological and nuclear materials is real. This further reinforces the urgent need to fully implement the Action Plan, with renewed focus on chemical threats.

Moreover, this Report also presents the state of play on the removal of **terrorist content online** following the March 2018 Commission Recommendation[6], as well as the Commission's way forward on **preventing radicalisation** following the final report of the High-Level Expert Group on Radicalisation. The 29 May 2018 Liège attack once again highlights the importance of the fight against radicalisation given that, according to the Belgian authorities, its perpetrator had been in contact with radicalised persons. This Report also identifies a number of actions to improve **passenger rail security**. Finally, this Report takes stock of the implementation of other priority files, notably the **interoperability of information systems** where two amending proposals – adopted by the Commission together with this Report – will allow the co-legislators to reach agreement before the end of the year. This Report also takes stock of the implementation of the **Passenger Name Record Directive** following the implementation deadline of 25 May 2018, actions to enhance cyber security and counter terrorist financing, as well as recent developments on the external dimension of security.

---

1 http://www.consilium.europa.eu/media/33457/22-euco-final-conclusions-en.pdf.
2 JOIN(2018) 16 final (12.6.2018).
3 JOIN(2018) 14 final (12.6.2018).
4 COM(2017) 610 final (18.10.2017).
5 Europol, Terrorism Situation and Trend report (TE-SAT) 2017, p. 16, available at: www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. See also the statements by the Director-General of the Organisation for the Prohibition of Chemical Weapons: www.globaltimes.cn/content/1044644.shtml.
6 C(2018) 1177 final (1.3.2018).

The Commission's **proposals for the Multiannual Financial Framework for 2021-2027** "A Modern Budget for a Union that Protects, Empowers and Defends"[7] also reflect that new security threats require new responses, underlining that security has an inherently cross-border and multi-sectorial dimension and therefore a strong, coordinated EU response is required. The Commission proposes to multiply the funding to internal security by factor 1.8 as compared to the current period 2014-2020. The elements responding to new security challenges are being set out in various sectorial legal proposals presented as part of the Multiannual Financial Framework.

II. ENHANCED PREPAREDNESS AGAINST CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR SECURITY RISKS

1. Progress in implementing the Action Plan

Chemical, biological, radiological and nuclear (CBRN) security threats are complex and can evolve rapidly, as demonstrated by the Salisbury nerve agent attack. Terrorist organisations have not used CBRN agents in Europe, but there are credible indications suggesting that they might have the intention of acquiring CBRN materials or weapons and are developing the knowledge and capacity to use them. The October 2017 Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks was presented in response to these threats, and focuses on pooling expertise and capabilities at EU level to improve operational preparedness across the Union. **Tangible progress** has been made in the implementation of the Action Plan, with measures taken across a number of areas to achieve the four objectives of the Action Plan: reducing the accessibility of CBRN materials; ensuring a more robust preparedness for and response to CBRN security incidents; building stronger internal-external links in CBRN security with key regional and international EU partners; and enhancing knowledge of CBRN risks.

First, as part of the efforts to reduce the accessibily of CBRN materials, the Union is stepping up **measures by customs authorities to prevent the illicit entry of CBRN materials**. Cargo information systems are essential to strengthen monitoring and risk-based controls of international supply chains. The Commission is therefore significantly upgrading the advance cargo information and customs risk management system by reshaping the existing loosely connected national systems into an integrated large-scale IT system. The new system will be centred on the common trade data repository capable to receive better quality real-time cargo information. It will inter-connect national customs authorities' risk assessment systems. The new system will be connected to thousands of additional parties involved in international logistics such as freight forwarders, logistic providers or postal operators across all modes of transport, providing the system with valuable cargo data that is not availabel today. The purpose of the system is to cover the full range of customs risks, including threats posed by CBRN materials.

Second, in terms of bolstering preparedness and resilience, Member States are enhancing their **capacity to detect CBRN materials** to help prevent CBRN attacks. At the Commission's initiative, a consortium of national experts carried out an **analysis of the gaps in detection equipment** for around 70 different types of CBRN scenarios. The gap analysis report has been shared and discussed with Member States, helping to guide future research needs and allowing them to make informed decisions on detection strategies and take operational measures to address the identified gaps. The analysis also shows a clear need for EU-wide

[7] COM(2018) 321 final (2.5.2018).

technical standards for detection equipment. Building on the results of the analysis, and using the framework of the CBRN Advisory Group[8] set up under the Action Plan, the Commission will work towards EU-wide standardisation for CRBN detection equipment. Moreover, Member States should establish inventories of stockpiles of essential medical countermeasures, laboratory, treatment and other capacities. The Commission will work with Member States to regularly map the availability of these stockpiles across the EU to increase their access and rapid deployment in case of CBRN attacks. Preparing and managing the consequences of a CBRN attack requires strengthened cooperation and coordination amongst Member States, including civil protection authorities. The Union's Civil Protection Mechanism can play a key part in this process with the aim of strengthening Europe's collective capacity to prepare and respond.

Third, the CBRN Action Plan emphasises the need for close **cooperation with key international partners and organisations**. On 28-29 June 2018, the Commission, in cooperation with the US Department of Energy, will organise an EU-US workshop on the security of radioactive sources. The Commission is also enhancing institutional and community capacities on CBRN in partner countries in the European Neighbourhood. Moreover, the Union is taking concrete steps to develop closer **cooperation with NATO** on CBRN, including on civil preparedness. EU representatives participated as observers in a workshop organised by NATO on civil-military cooperation in response to a large-scale CBRN terrorist attack. Moreover, the EU and NATO consider creating a joint awareness raising training module for decision-makers on CBRN. Moreover, the EU should explore measures to uphold respect for international rules and standards against the use of Chemical Weapons, including through a possible specific EU sanctions regime on Chemical Weapons. On the **transport side**, the Commission and Member States have been working with international partners to strengthen the preparedness of the EU Aviation Security system to tackle CBRN threats. This work has resulted in a list of actions to address CBRN threats against aviation.

Fourth, an effective response to CBRN risks requires expert knowledge at all levels, which makes it essential to step up the **pooling and sharing of expertise.** A best practice example is the Central European CBRN-E[9] Training Centre established in 2016 in Budapest by eight Member States.[10] It aims to share, enlarge and deepen first responders' CBRN-E knowledge, experiences and skills via trainings and exercises. Moreover, the Commission has positively evaluated a project proposal to strengthen this cooperation through the creation of a Mobile CBRN-E/Dirty Bomb First Responder Unit, deployable – upon request – in the case of a CBRN-E incident. The **area of forensics** is a case in point for the need to create collective capabilities. The collection of evidence and its processing in a contaminated area is highly challenging and requires specialised facilities**.** The Commission's Joint Research Centre is working on initiatives in this area with nuclear forensics capability in order to share specialised knowledge on related capabilities. Based on the results of the above-mentioned gap analysis, the Commission is also working with the CBRN Advisory Group in order to identify areas for the pooling of detection capabilities.

---

8 To facilitate cooperation between Member States, the Commission created a new **CBRN Security Advisory Group**, composed of national CBRN Security Coordinators. The Coordinators act as points of contact for the Commission on CBRN in each Member State. The Group, which has met in January 2018 for the first time, and will convene again in July 2018 to discuss developments on CBRN policy at EU level and coordinate the activities undertaken by Member States.

9 CBRN-E stands for chemical, biological, radiological, nuclear and explosives.

10 Czech Republic, Germany, Croatia, Hungary, Austria, Poland, Slovakia and Slovenia.

Fifth, **training and exercises** are ways to effectively share expertise on CBRN risks. Within the context of the EU-funded project eNotice, a database[11] listing over 200 relevant training initiatives has been made available, providing an overview of training opportunities across the Union. Member States are encouraged to use the available CBRN training opportunities to best effect. Moreover, making full use of the European Nuclear Security Training Centre, the Commission has launched a comprehensive training campaign for EU customs experts operating sophisticated radiation and nuclear detection equipment along the external borders, ports and airports. Moreover, the Commission has positively evaluated a project proposal for the development of a harmonised CBRN training curriculum for first responders and medical staff. In terms of practical exercises, in early 2018, the **Chimera table top exercise** organised by the Commission brought together the health, civil protection and security sectors throughout the EU to test cross-border preparedness and response planning on the basis of a fictitous scenario involving the deliberate release of a communicable disease. This EU-wide exercise contributed to the support of cross-sectoral capacity building and improved interoperability and coordination between health, civil protection and security sectors at EU and Member State level. Morever, the sharing of expertise also extends to the **private sector**, given the far-reaching consequences a CBRN attack can have on private sector operators. An industry-led project[12] aimed at raising awareness of security personnel mainly in the aviation sector, has produced an e-learning tool which gives essential information to those in contact with CBRN materials and agents.

2. Reinforced actions against chemical threats

The potential use of chemicals in terrorist attacks is increasingly prominent in terrorist propaganda. This adds to concerns that have arisen in relation to the terrorist plot uncovered in Australia in July 2017 and the use of chemicals in theatre recently. The Commission is therefore **fast-tracking further action on chemical threats** within the overall framework of the CBRN Action Plan, building on the progress made in terms of gap analysis on detection capacities and in the exchange of best practice in the CBRN Security Advisory Group.

A classified meeting with Member States' experts in March 2018 identified a number of urgent priorities for further cooperation against chemical threats. Building on that, the Commission will work with Member States to **complete the following steps** by the end of 2018:

- Develop a common list of chemical substances posing a particular threat, as a basis for further operational action to reduce their accessibility and enhance capabilities for their detection. This work will be carried out in a dedicated expert group set up in May 2018 on the detection of chemical threats, building upon on-going research in Member States and the Commission's Joint Research Centre.
- Set up a dialogue with private actors in the supply chain to work together towards measures to address developing and evolving threats from chemicals that can be used as precursors. This work follows the example[13] of the steps taken at EU level to

11 https://www.h2020-enotice.eu/static/roster.html.

12 The project was entitled "eTraining Against CBRN Terrorism: the development of a CBRN Online Training" (reference number - HOME/2013/ISEC/AG/CBRN/4000005269) and was financially supported under the Prevention of and Fight against Crime Programme.

13 As part of the work in the Security Union to close down the space in which terrorists and criminals operate, the Commission has taken firm action to reduce the access to explosives precursors that can be misused to make homemade explosives. In October 2017, the Commission presented a Recommendation setting out immediate actions to prevent misuse of explosive precursors based on existing rules

restrict the access to explosives precursors, and a first exchange of views already took place within the Standing Committee on Precursors.

- Accelerate a review of threat scenarios and an analysis of existing detection methods to improve the detection of chemical threats, with the aim of developing operational guidance for Member States to step up their detection capabilities. For that, the above-mentioned dedicated expert group has been set up to address the emerging chemical threats. In the longer term, the work of this group can pave the way towards standardisation of detection equipment.
- Raise awareness among first responders, in particular law enforcement and civil protection personnel, to enable them to recognise early signs of a chemical attack and react appropriately.

III. COUNTERING RADICALISATION

1. Countering terrorist content online

Addressing terrorist content online remains a key challenge in the prevention of radicalisation. Following the adoption of the Commission's Recommendation of 1 March 2018[14] on **tackling illegal content online**, a reporting exercise, as called for by the Recommendation, was subsequently initiated in order to monitor the efforts by both industry and Member States and other key partners such as Europol, in reducing accessibility to terrorist content online.

The initial findings from this first reporting exercise based on agreed indicators established within the EU Internet Forum – covering 13 companies in total and including the major social media companies[15], 20 Member States and Europol – indicate some progress on transparency, given that more information has been received from more companies, including from companies that had not previously engaged in the EU Internet Forum.

In addition, more companies are adopting proactive measures to identify terrorist content, and a higher volume of such content is being removed. Those who have developed automated tools to identify terrorist content (including content previously removed), have managed to improve the speed of removal of terrorist content on their platforms, whilst identifying and removing significant volumes of archived material. The Database of Hashes – a tool set up by a consortium of companies to facilitate co-operation so as to prevent the dissemination of terrorist content across platforms – continues to expand, both in terms of members and in terms of the amount of terrorist content captured in the database. 13 companies are now connected to the database, which now includes 80.000 image hashes and 8.000 video hashes. For the first time, some companies provided feedback on the impact of the Database of Hashes in terms of content removed, but this feedback needs to expand and become more detailed and systematic across platforms.

Referrals from Member States also remain an important component of the response. The number of Member States referring terrorist content to the internet companies continues to increase and Europol's Internet Referral Unit continues to seek ways to improve EU referrals – particularly in terms of co-ordinating and streamlining the process. The EU Internet Referral

---

(Recommendation C(2017) 6950 final of 18.10.2017). Building on that, the Commission adopted in April 2018 a proposal to revise and strengthen the existing Regulation 98/2013 on the marketing and use of explosives precursors (COM(2018) 209 final of 17.4.2018. See the Fourteenth progress report towards an effective and genuine Security Union (COM(2018) 211 final of 17.4.2018) for more details.

14 As reported in the Fourteenth Security Union Progress Report (COM(2018) 211 final of 17.4.2018).

15 Out of 33 companies contacted by the Commission.

Unit triggered 8.103 decisions for referrals in the fourth quarter of 2017, of which 89% were removed. In first quarter of 2018 5.708 decisions for referrals were triggered, to an increased number of smaller, less known, companies, with a 61% success rate. The removal success rates for those companies where there has been long-term engagement with the internet referral units, have remained stable – in most cases between 90% and 100%. The reported response speed by companies to referrals varies across platforms and ranges between under an hour to days, companies large and small need to further improve their response speed to respond adequately to the Recommendation to remove terrorist content within one hour of referral.

Full systematic feedback mechanisms on referrals are not yet in place, although Member States do acknowledge receiving receipts and some confirmation of action from several companies. Only one company provides full information on receipt, timing and action. To improve cooperation and coordination between law enforcement and companies, the EU Internet Referral Unit established in 2016 the Internet Referral Management Application. To date, three Member States are connected to the platform and others have expressed interest.

The Commission has launched an Impact Assessment to determine whether the current approach is sufficient, or whether additional measures are needed, in order to ensure the swift and proactive detection and removal of illegal content online, including possible legislative measures to complement the existing regulatory framework. The reporting under the Recommendation will feed into this assessment.

Europol's EU Internet Referral Unit led a multi-national co-ordinated effort to target Daesh's propaganda machine, involving six Member States as well as the United States and Canada. This collaborative effort – the culmination of over two years' worth of work involving 29 countries – not only delivered a significant disruption to Daesh's propaganda activities and infrastructure, but it also resulted in the seizure of a considerable volume of digital evidence.

2. Follow up to the High-Level Expert Group on Radicalisation

In parallel to the efforts to counter terrorist content online, the work at EU level continues to support the prevention of radicalisation in Member States and their local communities. The High-Level Expert Group on Radicalisation, established[16] in July 2017 to offer recommendations on how to improve coordination and collaboration between all relevant stakeholders, presented its **final report**[17] **on 18 May 2018**. It includes a broad range of recommendations for concrete action to address challenges in priority areas such as radicalisation in prisons (including follow up after release and the management of sentences), communication and online propaganda, multi-stakeholder cooperation at the local level, education and social inclusion, support to groups which require particular attention (including in particular as regards youth radicalisation and child returnees) as well as the external dimension. Recognising the added value and achievements of EU initiatives such as the Radicalisation Awareness Network (RAN), the European Strategic Communication Network (ESCN) and the EU Internet Forum, the report calls for strengthening these initiatives and the coordination between them, while creating closer links between all stakeholders involved, including front-line practitioners, policy makers and researchers. The report stresses the importance of actions at EU level being geared closer to Member States' needs.

16 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3552&NewSearch=1&NewSearch=1.

17 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3552.

The Commission welcomes the Final Report as it identifies areas that require urgent action, within Member States and at EU level. In particular, the Commission will follow up on the recommendation to establish an EU Cooperation Mechanism to ensure closer involvement of Member States in counter-radicalisation work. This EU Cooperation Mechanism will consist of a new Steering Board composed of Member States and a coordination and support structure on radicalisation to be set up in the Commission.

The Commission will take **immediate steps** to follow up on the recommendations of the Expert Group:

- First, by adopting a Decision to set up the Steering Board composed of Member States (with the EU Counter-Terrorism Coordinator and the European External Action Service as observers) to ensure that EU actions in this field are better geared towards needs and policy priorities within Member States and offering Member States the opportunity to be more closely involved in setting strategic orientations. A first meeting of the Board is envisaged at the latest in November 2018.
- Second, by setting up a reinforced coordination and support structure in the Commission in line with the limited resources currently available. Member States' contributions in building the required expertise would be particularly important to achieve the objectives set out by the Final Report. To this end, the Commission invites Member States to present proposals for cost-free secondments to the coordination and support structure. This will, together with the Steering Board, provide the EU Cooperation Mechanism on countering radicalisation.
- Third, by convening a meeting of the network of national prevent policy makers before October 2018 in order to facilitate further exchanges among Member States and to discuss concrete follow up actions.

The Commission takes note of the Expert Group's recommendation for an assessment and evaluation of the EU Cooperation Mechanism on countering radicalisation within 2019, and will aim to present the results of such an evaluation by December 2019, recognising that by that time the proposed measures may not have been fully implemented yet.

In the area of education, the Education, Youth, Culture and Sport Council adopted on 22 May 2018 a Recommendation[18] on the promotion of common values in schools to consolidate a stronger sense of belonging at local and national level, as proposed by the Commission.[19] This Recommendation calls on Member States to take further steps to **strengthen critical thinking and media literacy in schools**.

IV. CONCRETE SHORT-TERM MEASURES TO IMPROVE PASSENGER RAILWAY SECURITY

Transport hubs as well as railways and trains represent a high-risk target since the infrastructure is open by design[20]. Currently, 26 million passengers board European trains every day, with rail travel projected to increase by around 80% by 2050. Protecting rail users,

---

18 Council Recommendation on promoting common values, inclusive education, and the European dimension of teaching: http://data.consilium.europa.eu/doc/document/ST-8015-2018-INIT/en/pdf.

19 Thirteenth progress report towards an effective and genuine Security Union (COM(2018) 46 final of 24.1.2018).

20 Eleventh progress report towards an effective and genuine Security Union (COM(2017) 608 final of 18.10.2017).

workers and infrastructure from ever-evolving security threats is a crucial and on-going challenge. European rail transport needs to remain safe and secure.

Europe needs a **modern rail security system** that is based on risk assessment, and that allows a prompt and proportionate response to emerging threats whilst keeping rail services accessible. To deliver an increased level of security, keeping European railways accessible and open for passengers, and preventing unnecessary barriers to the internal market, Member States should improve information sharing and raise the level of awareness, preparedness and capacity to respond to terrorist incidents. Measures introduced by individual Member States without upstream coordination may create barriers and generate costs in terms of longer travel time, cancellations and overcrowded access to railway hubs.

There is a need for **equivalent levels of security for EU rail passengers across borders and transport operators.** Action at EU level to ensure cross-border coordination of all actors involved can contribute to consistent security protection across the EU.

The Commission is therefore suggesting to take a number of **concrete short-term actions to improve the security of rail passengers in the EU** (see Annex I)**.** The EU counter-terrorism package adopted on 18 October 2017 announced measures to enhance the protection of public spaces[21], and these actions builds upon this, and on dedicated studies showing that action should be taken to improve the security resilience of EU railways, particularly for international services.[22] These actions also reflect the outcomes of a risk assessment conducted by the Commission, Member States and EU INTCEN.

The identified actions are **both at EU and national level to enhance rail security.** At EU level, the Commission proposes the establishment of an EU Rail Passenger Security Platform, to create an effective cooperative environment and propose recommendations to help Member States coordinate rail security actions efficiently. The Platform will provide support in collecting and exchanging vital information on rail security, on optimising the security of cross-border rail services and defining a coordination mechanism to avoid unilateral decisions at national level. It will also help Member States and rail stakeholders jointly assess new threats and security incidents, and to undertake an appropriate coordinated response. In addition, the Commission, in close coordination with the Member States the European External Action Service and relevant agencies will develop a common risk assessment methodology for rail security risks at EU level.

The proposed actions will be tested in practice. The Commission will set up annual activities, testing the efficiency of this mechanism in different scenarios. This could be linked to existing EU sponsored exercises undertaken by railway police forces. The Commission will report on the implementation of these actions, and may consider all appropriate measures in line with Better Regulation principles in order to improve the actions or remedy any identified shortcomings.

V. IMPLEMENTATION OF OTHER PRIORITY FILES ON SECURITY

1. Towards the interoperability of information systems

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

[22] Steer Davies and Gleave, Study on options for the security of European high-speed and international rail services conducted at the request of the services of the EC, December 2016: http://europa.eu/!mM86yp.

Working towards stronger and smarter information systems for security, border and migration management, the EU is addressing shortcomings in EU information management and sharing as a matter of urgency and as a top priority. Central to this are the Commission's December 2017 proposals[23] on the interoperability of information systems that the European Parliament and the Council continue to examine. The three institutions have agreed, in the Joint Declaration on the EU's legislative priorities, on the shared objective of reaching agreement on the proposals before the end of 2018. For that reason, as previously announced[24], the **Commission tabled together with this report two amended proposals on interoperability** that incorporate the necessary amendments to the December 2017 interoperability proposals relating to those legal instruments that had still been under negotiation at the time. The Commission invites the co-legislators to include the amended proposals into their on-going examination of the interoperability proposals, with a view to enter into trilogues without delay.

The amended proposals reflect the recent progress made by the European Parliament and the Council on legislative proposals on EU information systems for security, border and migration management. The co-legislators reached final political agreement on 25 April 2018 on establishing the **European Travel Information and Authorisation System (ETIAS)**[25] that will allow for advance irregular migration and security checks of persons travelling visa-free to the EU. On 12 June 2018, the co-legislators also reached political agreement on the three legislative proposals[26] to strengthen the **Schengen Information System**, the most widely used information sharing system for security and border management in Europe. This will increase the security of European citizens by enhancing the ability of the system to fight terrorism and cross-border crime, improve border and migration management and ensure an effective information exchange between Member States. Moreover, the co-legislators reached political agreement on 24 May 2018 on the legislative proposal[27] to strengthen **eu-LISA, the European Agency for the operational management of large-scale IT Systems** in the area of freedom, security and justice. The reinforced mandate will enable the Agency to develop and roll out the technical solutions to make the relevant information systems interoperable. The agreement reached on these three initiatives, as well as the progress made in the discussions on the legislative proposal[28] to extend the **European Criminal Records Information System** to third-country nationals, allowed the Commission to present the above-mentioned amended proposals on interoperability, integrating the necessary amendments relating to those legal instruments into the December 2017 interoperability proposals.

The amended proposals on interoperability do not include the amendments relating to **Eurodac**, the EU asylum and irregular migration database, given that discussions have not yet

---

23 COM(2017) 793 final and COM(2017) 794 final (12.12.2017).

24 See the Fourteenth progress report towards an effective and genuine Security Union (COM(2018) 211 final of 17.4.2018). The December 2017 legislative proposals on the interoperability of information systems already include the necessary amendments to the legal instruments of the Schengen Borders Code, the future Entry/Exit System and the Visa Information System. They do not include the necessary amendments to other instruments (Regulations on the European Travel Information and Authorisation System, Eurodac, the Schengen Information System, the European Criminal Records Information System for third-country nationals and the European Agency for the operational management of large-scale IT System) that were under negotiation in the European Parliament and Council when the interoperability proposals were presented.

25 COM(2016) 731 final (16.11.2016).

26 COM(2016) 881 final, 882 final and 883 final (21.12.2016).

27 COM(2017) 352 final (29.6.2017).

28 COM(2017) 344 final (29.6.2017).

been concluded on the May 2016 legislative proposal[29] to strengthen Eurodac. The current architecture of the existing Eurodac system is technically unsuitable to become part of the interoperability of information systems given that it only stores biometric data and a reference number, but no other personal data (e.g. name(s), age, date of birth) that would allow for the detection of multiple identities linked to the same set of biometric data. The May 2016 legislative proposal seeks to extend the purpose of Eurodac to the identification of illegally staying third-country nationals and those who have entered the EU irregularly. In particular, it provides for the storage of personal data such as the name(s), age, date of birth, nationality, and identity documents. These identity data are essential to ensure that Eurodac will be able to contribute to the objectives of interoperability and function with its technical framework. This necessity underlines the need for the co-legislators to urgently reach agreement on the legislative proposal. Pending agreement on the legislative proposal to strengthen Eurodac, the data of illegally staying third-country nationals and those who have entered the EU irregularly could not be part of the interoperability of EU information systems. Once the co-legislators reach agreement on the legislative proposal to strengthen Eurodac, or have achieved sufficient progress, the Commission will present the related amendments to the interoperability proposals within two weeks.

On 16 May 2018, the Commission put forward a legislative proposal[30] to strengthen the **Visa Information System (VIS)** in order to better respond to evolving security and migratory challenges and improve the EU's external border management. While the existing Visa Information System is already covered by the interoperability proposals of December 2017, the May 2018 legislative proposal to strengthen the Visa Information System would enable the system to make full use of the proposed interoperability solutions. The proposal provides for enhanced checks across databases to prevent migration and security risks in issuing visas and for strengthened capacity to prevent crime, thus contributing to enhancing security and closing information gaps.

2. Implementation of the Passenger Name Record Directive

The **Passenger Name Records (PNR) Directive**[31] is crucial to the Union's common response to the threat of terrorism and organised crime. The deadline for Member States to implement the Directive expired on 25 May 2018. At the date of 7 June 2018, fourteen Member States have communicated to the Commission the measures they have adopted to transpose the Directive.[32] The remaining thirteen Member States have not yet notified their national transposition measures.[33] In nine Member States the necessary legislation has been tabled in parliament for adoption, while in another Member State primary legislation implementing the Directive has already been adopted, but the adoption of secondary legislation to reach full transposition is still pending. Among the Member States which have not yet notified transposition to the Commission, five have legislation in force which allows them to collect

29 COM(2016) 272 final (4.5.2016).

30 COM(2018) 302 final (16.5.2018).

31 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149.

32 Belgium, Croatia, Estonia, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Slovakia and the United Kingdom. Information about the national transposition measures communicated by the Member States is publicly available through Eur-Lex: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32016L0681.

33 Denmark does not take part in the PNR Directive.

PNR data under national law. However, their legislative framework still needs to be amended in order to fully comply with the Directive.

In addition to the communication of national transposition measures under Article 18, the PNR Directive foresees specific notifications concerning its application to intra-EU flights (Article 2); the setting up of Passenger Information Units (Article 4) and the list of competent authorities entitled to request and receive PNR data from the PIU (Article 7). All twenty-seven Member States[34] have sent to the Commission the list of their competent authorities entitled to request or receive PNR data or the result of processing those data, as provided for by Article 7(3) of the PNR Directive. Nineteen Member States have informed the Commission that they intend to apply the Directive to intra-EU flights as per Article 2(1) and another twenty-one have notified the establishment of their Passenger Information Unit (PIU) under Article 4(5).

Besides taking steps to transpose the Directive into national law and complete the necessary institutional arrangements, Members States have achieved progress in establishing the technical solutions needed for the storage, processing and analysis of PNR data. Twenty-four Member States have a PNR technical solution in place, while the remaining three are at various stages of deployment for the necessary infrastructure. The process to establish connectivity with air carriers for the purposes of enabling the transmission of PNR data to the PIUs is well-advanced in twelve Member States, while in an additional eleven at least one air carrier is already transmitting real-time PNR data to the PIU.

Overall therefore, the Commission notes that significant progress has been achieved in the implementation of the PNR Directive over the past two years. However, given the crucial importance of this instrument for the EU's common response to terrorism and serious crime, the Commission will make use of all the measures at its disposal for the enforcement of EU law, including infringement action when appropriate. Lack of transposition hampers the effectiveness of the EU PNR mechanism on the whole, reduces legal certainty for air carriers by delaying the creation of a single, EU-wide regime for providing PNR data, and hampers the effective protection of personal data across the EU. The Commission will continue to support all Member States in their efforts to complete the development of their PNR systems, including by facilitating the exchange of information and best practices after the implementation deadline. In this regard, a first meeting with Member States to discuss issues related to the application of the PNR Directive took place on 7 June 2018.

3. Cybersecurity and cyber-enabled threats

The Commission continues, in cooperation with the European External Action Service, to implement the actions set out in the September 2017 Joint Communication[35] on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU".

9 May 2018 marked the deadline for all EU Member States to transpose the **Directive on Security of Networks and Information Systems** in national law. It is the first EU-wide legally binding set of rules on cybersecurity, which establishes a high common level of security of network and information systems across the EU.

On 6 and 7 June 2018, the 5th **pan European cyber crisis exercise Cyber Europe 2018** took place under the coordination of the EU Agency for Network and Information Security

34 Denmark does not take part in the PNR Directive.
35 JOIN (2017) 450 final (13.9.2017).

(ENISA).[36] The exercise was organised for IT security, business continuity and crisis management teams coming from EU and EFTA Member States, and involved more than 1000 participants. The scenario revolved around Aviation, potentially involving Civil Aviation Authorities, Air Navigation Service Providers (ANSPs), Airport Companies, Air Carriers, with potential impacts in other sector.

The exposure of citizens to large-scale disinformation, including misleading or outright false information, is another serious type of cyber-enabled threat and a major challenge for Europe. In its Communication of 26 April 2018 "**Tackling online disinformation: a European approach**"[37], the Commission put forward an action plan and self-regulatory tools to tackle the spread and impact of online disinformation in Europe, and ensure the protection of European values and democratic systems. The specific measures presented include an EU-wide Code of Practice on Disinformation for online platforms and advertisers, support for an independent network of fact-checkers, and a series of actions to stimulate quality journalism and promote media literacy. A first meeting of the Multi-stakeholder Forum on Disinformation was held on 29 May 2018 and committed to an ambitious roadmap to ensure adoption of the Code on 17 July 2018.

The Internet Corporation for Assigned Names and Numbers (ICANN) plays a key role in supporting the public policy objectives of the Domain Name System. The Commission recalls[38] that ICANN should accelerate its efforts to make sure it fully complies with the General Data Protection Regulation as a result of the ongoing reform of the **WHOIS service**, while ensuring a WHOIS model that preserves essential public interest functions, ranging from law enforcement to cybersecurity and intellectual property rights protection. With this objective in mind, the Commission is continuing to facilitate discussion between ICANN and the European Data Protection Board[39] (EDPB) with a view to establishing a new model which fulfils both objectives. In that regard, the Commission calls on ICANN to take responsibility for the resolution of their pending issues. On 17 May 2018, the ICANN Board adopted a Temporary Specification for gTLD Registration Data (so-called generic top level domains) that applies from 25 May 2018 with the aim to ensure compliance with the GDPR. Although the Temporary Specification leaves open a number of issues including in relation to access to WHOIS data for legitimate purposes, such as for law enforcement investigations, the ICANN Board committed to continue working together with the community to develop and implement a comprehensive and permanent solution.[40] On 27 May 2018, the European Data Protection Board endorsed a statement that recognises efforts undertaken by ICANN to ensure the compliance of the WHOIS system with the GDPR, although further progress by ICANN to ensure that legal requirements are properly addressed will continue to be monitored.[41] As the absence of a comprehensive model for the WHOIS service may seriously hamper the ability of law enforcement authorities to investigate crimes, including cybercrimes, the Commission will also remain vigilant that an appropriate model that provides for access to WHOIS data for legitimate purposes is delivered in time by ICANN.

---

36 For more details see: http://www.cyber-europe.eu/.

37 COM(2018) 236 final (26.4.2018).

38 In the fourteenth Security Union Progress Report (COM(2018) 211 final of 17.4.2018), the Commission reported on ongoing developments regarding the WHOIS service notably in view of the application of the General Data Protection Regulation from 25 May 2018.

39 Replacing the Article 29 Working Party.

40 The ICANN Board confirmed this approach in a letter to the Commission on 23 May 2018: https://www.icann.org/resources/pages/correspondence.

41 https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois_sv.

4. Countering money laundering and terrorist financing

Given that criminals and terrorists operate across different Member States and are able to transfer funds between different bank accounts in a matter of hours to prepare their acts or to move and launder proceeds of crime, countering money laundering and terrorist financing is an important aspect of the work towards an effective Security Union. On 14 May 2018, the Council adopted a Directive strengthening EU rules to prevent money laundering and terrorist financing. The so-called **5th Anti-Money Laundering Directive** will increase transparency about the ownership of companies and trusts to prevent money laundering and terrorist financing via opaque structures. It will improve the work of Financial Intelligence Units with better access to information through centralised bank account registers. It will also tackle terrorist financing risks linked to the anonymous use of virtual currencies and pre-paid instruments. Finally, it will ensure a common high level of safeguards for financial flows from high-risk third countries.

On 30 May 2018, European Parliament and the Council reached a political agreement on the legislative proposal[42] for a Directive to **counter money laundering by criminal law** that will harmonise money laundering criminal offences.

In the context of the Action Plan[43] for strengthening the fight against terrorist financing, the Council called on the Commission in February 2016 "to explore the need for appropriate restrictions on cash payments exceeding certain thresholds". Following this, the Commission informally consulted Member States, commissioned a study to an external contractor and conducted a public consultation between March and May 2017. The Commission published a **Report on restrictions on payments in cash** together with this Security Union progress report. The findings have led to the conclusion that restrictions on payments in cash would not significantly hinder terrorism financing, but that such restrictions could be useful in combatting money laundering. The Commission will not at this point take further legislative action on this matter.

5. External dimension

Small Arms Light Weapons (SALW) and illicit firearms continue to contribute to instability and violence, both in the European Union, its immediate neighbourhood and beyond. The Commission and the High Representative therefore propose to the Council a revision of the 2005 Small Arms Light Weapons Strategy, taking into account the new security context, EU initiatives and developments in conventional arms control that have taken place since 2005, namely: the entry into force of the Arms Trade Treaty, the conclusion of the UN Firearms Protocol, the revision of the EU legislation on firearms, the activities with neighbouring countries through the Commission's Action Plan of 2015[44] and the work done in the context of the EU Policy Cycle. This updated strategy aims to guide collective and coordinated European Action to prevent and curb the illicit acquisition of firearms and small arms and light weapons, and their ammunition by terrorists, criminals and other unauthorised players. The Strategy supports reinforced international and EU-level norms, improved controls and the traceability of firearms, small arms and light weapons and ammunitions during their life-cycle.

---

42 COM(2016) 826 final (21.12.2016).
43 COM (2016) 50 (2.2.2016).
44 COM(2015) 624 final (2.12.2015).

On 23-24 April 2018, the **G7 Security Ministers** met in **Toronto** to discuss G7 security cooperation, including common action against developing terrorist threats. The Toronto Commitments of the Security Ministers[45] put a focus on the protection of public spaces, the preparedness against CBRN risks and efforts to counter terrorist content online, enhance cyber security and counter trafficking in human beings. A joint session of Security Ministers and Foreign Ministers resulted in the adoption of joint commitments on managing foreign terrorist fighters and associated travellers[46] and on defending democracy and addressing foreign threats[47].

On 14 May 2018, the Council adopted a decision allowing for the EUNAVFOR MED Operation Sophia to host the pilot project "**Crime Information Cell**" (CIC). The CIC will be located on the ship hosting the force headquarters of Operation Sophia, as a hub within the Operation, where all relevant actors can work together to facilitate the receipt, collection and timely and two-way exchange of information for analytical and further operational use between EUNAVFORMED Operation Sophia, relevant Justice and Home Affairs Agencies and Member states' law enforcement authorities, on issues related to the Operation mandate, namely migrant smuggling, human trafficking, arms trafficking, illegal trafficking of oil exports and for force protection of the Operation.

The Sofia Summit with **Western Balkans leaders** took place on 17 May 2018. It confirmed the European perspective of the region and set out a number of concrete actions to strengthen cooperation, including importantly in the areas of security and the rule of law, in line with the Security and Migration Flagship of the Western Balkans Strategy.[48]

On 22 and 23 May 2018, the **EU-US Ministerial Meeting on Justice and Home Affairs** was hosted by Bulgarian Council Presidency in Sofia. The EU and US discussed efforts to combat terrorism, focusing on effective information sharing, preventing radicalisation, use of the internet for terrorist purposes, and vigilance with respect to chemical, biological, radiological and nuclear threats, especially in relation to the evolving chemical threats to aviation security and public spaces.

On 25 May 2018, the first **EU-UN Dialogue on Counter Terrorism** at high level took place in Brussels. The EU and the UN discussed efforts to cooperate on preventing and countering terrorism on a focused number of thematic and geographic priorities, with a focus on foreign terrorist fighters and victims of terrorism.

On 29 May 2018, staff from the **EU** and **NATO** held a first **Counter-Terrorism Dialogue** in Brussels in the framework of the ongoing implementation of their 2016 Joint Declaration. They addressed the challenges of retuning or relocating foreign terrorist fighters and counter-terrorism capacity building efforts in Iraq, Afghanistan, Bosnia-Herzegovina and Tunisia.

---

45 https://g7.gc.ca/en/g7-presidency/themes/building-peaceful-secure-world/g7-ministerial-meeting/chairs-statement-security-ministers-meeting/g7-security-ministers-commitments-paper/.

46 https://g7.gc.ca/en/g7-presidency/themes/building-peaceful-secure-world/g7-ministerial-meeting/managing-foreign-terrorist-fighters-associated-travellers/.

47 https://g7.gc.ca/en/g7-presidency/themes/building-peaceful-secure-world/g7-ministerial-meeting/defending-democracy-addressing-foreign-threats/.

48 COM(2018) 65 final (6.2.2018). This includes: stepping up joint work on counter-terrorism and prevention of radicalisation, enhancing the cooperation in the fight against organised crime in priority areas such as firearms, drugs, migrant smuggling and trafficking in human being and preparing a renewed actions plan on cooperation against illicit firearm trafficking.

On 4 June 2018, the Justice and Home Affairs Council adopted eight Decisions authorising the Commission to open negotiations for agreements between the EU and **Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey respectively on the exchange of personal data between Europol and those countries**' competent authorities for fighting serious crime and terrorism.

Following the recent adoption of a negotiating mandate by Canada at the end of May 2018 for a **revised Passenger Name Record Agreement between the EU and Canada**, the Commission and Canada have immediately taken steps to launch formal negotiations to that end and the opening of negotiations is scheduled for 20 June 2018.

VI. CONCLUSION

This report illustrates the continued progress made towards an effective and genuine Security Union, supporting Member States in countering terrorism, serious crime and cyber-enabled threats, and contributing to a high level of security for citizens. The Commission calls on the co-legislators to reach swift agreement on all those legislative proposals currently under discussion that seek to enhance further the security of citizens, in line with the Joint Declaration on the EU's legislative priorities for 2018-19.

The Commission will continue this work as a matter of priority, also in view of the informal meeting of Heads of State or Government on internal security in Salzburg on 20 September 2018 as part of the Leaders' Agenda.

EUROPEAN
COMMISSION

Brussels, 13.6.2018
COM(2018) 470 final

ANNEX

ANNEX

to the

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

Fifteenth Progress Report towards an effective and genuine Security Union

FURTHER MEASURES TO IMPROVE PASSENGER RAILWAY SECURITY

I. Actions by the European Commission

1. By the end of 2018, the Commission will establish an **EU Rail Passenger Security Platform**. This Platform will collect relevant information on rail security and provide good practice guidance for Member States. It will assess emerging security threats and incidents, and propose an appropriate response. The Platform will be composed of experts from Member States and will facilitate information sharing and expertise at European and national level.

2. By the end of 2018, the Commission will adopt a **common methodology for the assessment of rail security risks** at EU level, and it will keep this methodology up-to-date. Building on an initial assessment of security risks to the railway sector carried out by a Commission expert group in 2017, the Commission will develop a regular assessment and exchange of information concerning international rail services.

3. By the end of 2019, the Commission will adopt **technical guidance based on the work of the EU Rail Passenger Security Platform**. Where appropriate, the Commission will endorse the technical work of the platform in the form of technical guidance documents. Targeted areas for action are: (a) information to be provided to passengers in case of a security incident, (b) security technology and design solutions adapted to the specificities of the rail sector, and (c) staff scrutiny procedures and appropriate security training.

II. Actions by the Member States

4. By the end of 2018, Member States are invited to appoint a **national contact point on rail security** for all companies operating on the respective Member State's territory. A clear official link for cooperation between law enforcement authorities and railway undertakings, station and infrastructure managers, the national contact points will help ensure that security measures will take into account the specificity of the railway sector.

5. By the end of 2018, Member States are invited to implement a **mechanism at national level for sharing relevant information on rail security domestically and with other Member States** through the EU Rail Passenger Security Platform. To this end, the Commission invites Member States to make the necessary arrangements for the immediate sharing of relevant information on rail security between the different national authorities, with rail stakeholders and other Member States.

6. By the first half of 2019, Member States are invited to adopt a **programme for rail security management at national level**, identifying responsibilities and including protection and mitigation measures based on an analysis and assessment of risk. Security measures should be scalable according to changes to defined national threat levels.

7. By the end of 2019, Member States are invited to **require railway undertakings and infrastructure and station managers to adopt a security management plan** at company level, based on an analysis and assessment of risk, and proportionate to national threat levels.