EUROPEAN
COMMISSION

Brussels, 29.6.2017
COM(2017) 354 final

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

Eighth progress report towards an effective and genuine Security Union

I. INTRODUCTION

This is the eighth monthly 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 recent weeks, Europe has once again been hit by a series of terrorist attacks. On 22 May 2017, Manchester was the victim of a heinous terrorist attack when a bomb was activated outside a concert hall, killing 22 persons many of them teenagers. Twelve days later, on 3 June 2017, London was once again attacked when terrorists ploughed indiscriminately into pedestrians crossing London Bridge before carrying on their murderous assault on foot with knives in nearby Borough Market. On 18 June a similar van attack outside a mosque killed and injured innocent worshipers. Most recently on 19 June 2017, a terrorist tried to attack police officers on the Avenue des Champs-Élysées in Paris but was shot dead. On 20 June 2017, Belgian security forces shot dead an attempted suicide bomber at Brussels Gare Central whose bomb had failed to detonate. The volume and tempo of these attacks once again highlight the vital importance of fighting violent extremism and the challenge facing Member States both in thwarting attacks and in preventing and countering the radicalisation that fuels them.

This report sets out the measures taken at EU level to **prevent and counter radicalisation**, taking stock of the progress made in response to the challenges of radicalisation one year after the adoption of the June 2016 Commission Communication supporting the prevention of radicalisation leading to violent extremism[1]. The report also provides an update on progress made in the implementation of other priority files on security, with the next steps taken to enhance the **exchange of information** through the interoperability of information systems and to implement the Action Plan on terrorist financing[2] to **detect and prevent terrorist funding**.

The European Council conclusions[3] of 22-23 June 2017 reiterated and reinforced the Union's resolve to cooperate to fight the spread of radicalisation online, to coordinate the work on preventing and countering violent extremism and addressing the ideology, to thwart the financing of terrorism, to facilitate swift and targeted exchanges of information between law enforcement authorities, including with trusted partners, and to improve the interoperability between databases. The recent Taormina G7 Summit statement[4] on the fight against terrorism and violent extremism sent a strong signal of the international resolve to tackle the growing menace of terrorism and underlined the need for further concerted action at global level.

Finally, this report also addresses the **increased cyber threat** and sets out short-term actions to counter it, drawing on the lessons learned from the reaction to the *WannaCry* attack.

II. EU ACTION SUPPORTING THE PREVENTION OF RADICALISATION

Although violent radicalisation is not a new phenomenon, recent terrorist attacks in the EU have shown both the alarming speed and scale at which some EU citizens have become

1 COM(2016) 379 final (14.6.2016).
2 COM(2016) 50 final (2.2.2016).
3 http://www.consilium.europa.eu/en/meetings/european-council/2017/06/22-23-euco-conclusions_pdf/.
4 http://www.consilium.europa.eu/en/press/press-releases/2017/05/26-statement-fight-against-terrorism/.

radicalised. Terrorist recruiters deploy a range of different techniques to target the vulnerable. The use of digital communication tools presents new and particular challenges for Member States authorities. Countering radicalisation through a multi-faceted EU-level response, both on-line and off-line, therefore plays a key role in supporting Member States in countering terrorism.

To counter **radicalisation online**, the Commission has been working over the last two years with key internet platforms including under the EU Internet Forum to ensure the voluntary removal of online terrorist content. In these activities real progress has been made in removing terrorist content online[5] and countering illegal hate speech online[6], but there is still much more to do. The European Council conclusions of 22-23 June 2017 set out that "*building on the work of the EU Internet Forum, the European Council expects industry to establish an Industry Forum and 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 Commission hosted a Senior Officials Meeting of the EU Internet Forum on 27 June 2017 to agree further action with key internet service providers to combat terrorist content online. The **aim is that internet platforms do more**, notably to step up the automated detection of terrorist content, to share related technology and tools with smaller companies, and to make full use of the 'database of hashes' including by providing Europol with access to key information and establish a reporting system on removed terrorist content. In addition, to complement the work done by Europol's Internet Referral Unit, the Commission calls on all Member States to establish **national Internet Referral Units** and develop a network between them for joint engagement with internet platforms and Europol's Internet Referral Unit.

As witnessed by recent attacks, the unprecedented scale of radicalisation also requires further action to support prevention and anti-radicalisation at national and local level. The Commission will swiftly establish[7] a **High-Level Expert Group on Radicalisation** to facilitate the further development of EU policies in this area. The Group will be tasked with giving impetus to further work in high priority areas such as prison radicalisation, online terrorist propaganda, and returning Foreign Terrorist Fighters. The work of the Group will aim to bolster the **Radicalisation Awareness Network (RAN)** which has been at the forefront of the Commission's work to support Member States in this area, working with local practitioners at community level.[8] Most recently, on 19 June 2017, the network presented a **"Responses to Returnees" manual** to support Member States in addressing the challenges posed by returning Foreign Terrorist Fighters. This manual provides an overview of

---

5 Through Europol's **Internet Referral Unit** (IRU), 30.000 pieces of terrorist material have been referred to the internet platforms, with an average removal rate of 80-90%. Moreover, the internet industry-led initiative to create a **'database of hashes'** ensures that once terrorist material is taken down on one platform, it is not uploaded on another platform.

6 The Commission agreed in May 2016 on a **Code of Conduct countering illegal hate speech online** signed by Facebook, YouTube, Twitter and Microsoft, committing to review and remove content upon notifications of illegal hate speech quickly and efficiently. One year after its adoption, the Code has delivered significant progress. The companies have removed content in twice as many cases of illegal hate speech, and at a faster rate, as compared to before the agreement on the Code.

7 The Commission will establish this Group in July 2017.

8 The Radicalisation Awareness Network has offered training and advice to Member States, and developed a large number of best practices, guidelines, handbooks and recommendations. Themes and issues covered include polarisation, prison radicalisation and exit programmes, family support measures, youth work and education, community policing, communication and narratives, engagement and empowerment of young people.

approaches from practitioners to address different scenarios of persons returning from conflict zones. In the coming months, the network will organise a series of workshops for national authorities to elaborate further on these practices and encourage action in the Member States.

The complex challenges around radicalisation require a multi-faceted response including long-term measures, as set out in the June 2016 Communication on preventing radicalisation leading to violent extremism.[9] Over the last year, the Commission has implemented most of the **key actions identified in other areas related to prevention and anti-radicalisation**.[10] To support Member States in addressing radicalisation in prison, a dedicated Prison and Probation Group under the Radicalisation Awareness Network was set up to provide guidance to front-line practitioners such as prison and probation staff, psychologists and religious representatives. Education plays a key role in preventing radicalisation, and the Commission has taken a series of steps to implement the Paris Declaration on promoting citizenship and the common values of freedom, tolerance and non-discrimination through education. The Erasmus+ programme is central in that respect.[11] Given the links between marginalisation, vulnerability and radicalisation, the European Pillar of Social Rights[12], adopted on 26 April 2017, is an important element in addressing some of the root causes of radicalisation and violent extremism.[13] To strengthen the cohesion of European societies, the Commission is also implementing the Action Plan on the integration of third country nationals[14] with a wide set of measures to support Member States and other actors in their integration efforts.

On the **external side**, the EU is working in international fora – notably the Organization for Security and Co-operation in Europe (OSCE) and institutions[15] flowing from the Global Counter Terrorism Forum – to support prevention and anti-radicalisation in partner countries in the Western Balkans, the Middle East and North Africa region, including training of relevant professionals and financial support for grass-roots initiatives engaging in prevention efforts. A new Erasmus+ Virtual Youth Exchange initiative will be launched in 2018 to

---

9 See table in Annex 1 listing the action taken to implement the June 2016 Communication.

10 The June 2016 Communication focuses on **seven specific areas**: (1) supporting research, evidence building, monitoring and networking; (2) countering terrorist propaganda and hate speech online; (3) addressing radicalisation in prisons; (4) promoting inclusive education and EU common values; (5) promoting an inclusive, open and resilient society and reaching out to young people; (6) the security dimension of addressing radicalisation; and (7) the international dimension.

11 Under the **Erasmus+ programme**, in 2016 more than EUR 200 million were devoted to developing new policy approaches and practices through 1200 transnational partnership projects, involving local actors and with a focus on inclusive education, youth work, citizenship and intercultural education. A new toolkit, developed in cooperation with Member States' experts, provides youth workers with guidance and advice when working with young people at risk of violent radicalisation. The Commission also launched a **Role models network** implemented through Erasmus+. This initiative will allow local actors to benefit from small amounts of EU funding to set up pools of role models to embark in activities to promote social inclusion among pupils and young people.

12 https://ec.europa.eu/commission/priorities/deeper-and-fairer-economic-and-monetary-union/european-pillar-social-rights/european-pillar-social-rights-20-principles_en.

13 In May 2017, the Commission launched an online public consultation with a view to prepare a proposal for a Council Recommendation on promoting social inclusion and shared values before the end of 2017. The aim is to establish a policy framework to support Member States in promoting inclusive education that fosters ownership of shared values, contributing to preventing radicalisation leading to violent extremism.

14 COM(2016) 377 final (7.6.2016).

15 The Global Community Engagement and Resilience Fund (GCERF), the Hedayah Centre of Excellence on Countering Violent Extremism and the International Institute for Justice and the Rule of Law.

increase intercultural awareness and understanding between young people inside and outside the EU. The Radicalisation Awareness Network also deployed experts to support preventive action in Turkey, the Western Balkans and Tunisia.

III. EU ACTION ADDRESSING CYBER THREATS AND CYBERCRIME

The May 2017 *WannaCry* ransomware attack was a wake-up call highlighting gaps in the current cybersecurity framework, notably in terms of preparedness and cooperation. As announced already before the attack, in the Digital Single Market mid-term review, **the Commission is accelerating its work on cybersecurity**, including through its review of the 2013 Cybersecurity Strategy. The Commission and the European External Action Service are assessing progress made in implementing the current Strategy. The aim is to identify gaps that will be addressed in the review of the Strategy in September 2017.

In parallel to that and responding to the lessons learned from the reaction to the *WannaCry* attack, a number of **short-term actions** should now be taken to strengthen our response to the increased cyber threat. This includes the need to move forward quickly to strengthen our resilience, especially on issues relating to operational cooperation.

The *WannaCry* attack was the first incident prompting cooperation in the **network of national Computer Security Incident Response Teams** (CSIRT network) established under the **Network Information Security (NIS) Directive**. The incident demonstrated that the system was not yet fully operational. It also showed a clear need to accelerate the on-going work to improve existing IT tools, and deploying additional capabilities to enable further cooperation among national CSIRTs. To strengthen these teams, the Commission will provide funding of EUR 10.8 million to 14 Member States under the Connecting Europe Facility, with two-year projects starting by September 2017. Another call for proposals is currently open and all remaining Member States are invited to submit their funding applications.

Europol's **European Cybercrime Centre** (EC3) led the law enforcement response to this attack. To strengthen the centre and the services it provides, it is necessary to equip it with further IT expertise. For that, Europol's Management Board should improve by September 2017 the possibilities for the recruitment of IT specialists under Europol's internal rules. This work at Europol will be further supported with additional staff in 2018.

The **EU Computer Emergency Response Team** (CERT-EU) supports EU Institutions to protect themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and harm the interests of the EU. The Commission will now accelerate the formal process of putting CERT-EU on a stronger footing, by concluding arrangements between the relevant institutions and bodies in order to strengthen the collective response to threats. This includes the European Parliament, the Council, the Court of Justice of the European Union, the European Central Bank, the Court of Auditors, the European External Action Service, the Economic and Social Committee, the Committee of the Regions, and the European Investment Bank. The Commission will shortly sign an inter-institutional administrative agreement with the other institutions and bodies.

These short-term actions are part of the wider **review of the 2013 Cybersecurity Strategy** that will follow in September 2017, accompanied by the necessary action to reinforce the Union's cyber resilience and security. The European Council conclusions of 22-23 June 2017

welcome the Commission's intention to review the Cybersecurity Strategy in September and to propose further targeted actions before the end of the year.

Successful deterrence also requires effective traceability, detection, investigation and prosecution. Access to **electronic evidence** is a key issue in this respect. Criminal justice frameworks currently still reflect traditional concepts of territoriality and are challenged by the cross-jurisdictional nature of electronic services and data flows. The European Council conclusions of 22-23 June 2017 underline that effective access to electronic evidence is essential to combating serious crime and terrorism and that, subject to appropriate safeguards, the availability of data should be secured. At the Justice and Home Affairs Council on 8 June 2017, Ministers expressed broad support for practical measures proposed by the Commission to improve the situation within the current legislative framework. Ministers also invited the Commission to present a legislative proposal as soon as possible, bearing in mind the technical and legal challenges. On that basis, the Commission will continue to implement practical measures and while working on an impact assessment to inform possible future legislative action to be presented as soon as possible.

Encryption is an equally important issue in this context. Encryption is vital for the protection of cybersecurity and personal data. Its abuse by criminals, however, creates significant challenges in the fight against serious forms of crime, including cybercrime and terrorism. The European Council conclusions of 22-23 June 2017 call for addressing the challenges posed by systems that allow terrorists to communicate in ways that competent authorities cannot access, including end-to-end encryption, while safeguarding the benefits these systems bring for the protection of privacy, data and communication. As requested by the Justice and Home Affairs Council in December 2016, the Commission is working closely with EU agencies and industry to identify how to support law enforcement authorities in overcoming the most significant challenges, taking into account the implications for cybersecurity and fundamental rights. Together with Europol, Eurojust, the EU Network and Information Security Agency (ENISA) and the EU Fundamental Rights Agency, the Commission discussed all aspects of this important matter with relevant experts in a series of workshops. The Commission will report its findings to the European Parliament and the Council by October 2017.

On the **external side**, the Council agreed on 19 June 2017 to develop a framework for a joint EU diplomatic response to malicious cyber activities, the **cyber diplomacy toolbox**.[16] The framework for a joint EU diplomatic response will make full use of measures within the Common Foreign and Security Policy, including, where necessary, restrictive measures. Any joint EU response to malicious cyber activities should be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity. The framework seeks to encourage cooperation, facilitate mitigation of immediate and long-term threats, and influence the behaviour of potential aggressors in the long term. Together with Member States, the Commission and the European External Action Service will put in place implementing guidelines in the months to come, including preparatory practices, communication procedures and exercises.

[16] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf .

IV. IMPLEMENTATION OF OTHER PRIORITY FILES ON SECURITY

1. Next steps towards the interoperability of information systems

As set out in the seventh progress report,[17] the Commission is taking further action to implement the new approach to the management of data for borders and security. On 28 June 2017, the Commission presented a **legislative proposal[18] to strengthen the mandate of eu-LISA**.[19] The agency will play a crucial role in the technical work towards the interoperability of information systems, including with ongoing technical analysis on the identified solutions to achieve this. Subject to the adoption of the relevant legislative proposals by the co-legislators, the proposed changes to its mandate will give eu-LISA responsibility for the development of interoperability solutions, thus ensuring the technical implementation of this new approach. The European Council conclusions of 22-23 June 2017 indicate the importance of the interoperability of information systems for internal security and the fight against terrorism.

The Commission also presented on 28 June 2017 a supplementary proposal to its January 2016 proposal[20] to facilitate the **exchange of criminal records of third-country nationals** in the EU through the European Criminal Records Information System (ECRIS).[21] This supplementary proposal responds to the discussions with the co-legislators on last year's proposal and is part of the Commission's approach on the interoperability of information systems. The improvement of the ECRIS with regard to information exchange on third-country nationals is a legislative priority identified in the Joint Declaration[22] of the Presidents of the European Parliament, the Council and the Commission.

There is also **progress on other priority files on information systems**. Discussions continued between the co-legislators on the proposed EU Entry/Exit System[23], with trilogue meetings held on 31 May, and 13, 19 and 26 June 2017. The Council agreed on a general approach on the proposed European Travel Information and Authorisation System (ETIAS)[24] at the Justice and Home Affairs Council on 8/9 June 2017. The vote in the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) on the tabled amendments to the proposal is scheduled for September 2017, and trilogue negotiations are expected to start in October 2017. It is essential that the European Parliament and the Council move forward on these priority proposals, as again underlined in the European Council conclusions of 22-23 June 2017.

On 29 May 2017, the Commission, together with the European Data Protection Supervisor, the EU Fundamental Rights Agency and the EU Counter-Terrorism Coordinator, presented to the LIBE Committee the findings of the High-level Expert Group on Information Systems and Interoperability[25] and the Commission's new approach to the management of data for

---

17 COM(2017) 261 final (16.5.2017).
18 COM(2017) 352 final (29.6.2017).
19 European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.
20 COM(2016) 7 final (19.1.2016).
21 COM(2017) 344 final (29.6.2017).
22 https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-legislative-priorities-2017-jan2017_en.pdf.
23 COM(2016) 194 final (6.4.2016).
24 COM(2016) 731 final (16.11.2016).
25 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

borders and security. On 8 June 2017, the Council adopted conclusions[26] on information exchange and interoperability, welcoming the Commission's views and the proposed way forward to achieve the interoperability of information systems by 2020 on the basis of the recommendations of the High-level Expert Group. Building on these discussions, the Commission will further work with the European Parliament and the Council to achieve the interoperability of information systems by 2020.

2. EU Action to cut off sources and channels of terrorist financing

Work is on-going to implement the February 2016 **Action Plan on terrorist financing** along two main strands of action: to detect and prevent terrorist funding, and to disrupt the sources of revenues. In December 2016, the Commission presented three legislative proposals to complete and reinforce the EU legal framework in the areas of money laundering[27], illicit cash flows[28] and freezing and confiscation of assets.[29] The Commission calls on the co-legislators swiftly to advance the work on these important proposals.

In addition, the co-legislators made considerable progress in the negotiations on the amendments to the **4th Anti-money Laundering Directive**, based on a legislative proposal of July 2016.[30] The Commission remains fully committed to a swift finalisation of the on-going trilogues. Taken together, these measures **complete the commitments the Commission had undertaken to do in the Action Plan**.[31] They will also ensure the EU meets its international obligations in this area as agreed in the context of the Financial Action Task Force (FATF) and Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (Warsaw Convention).

As set out in the Action Plan, the Commission also intends to adopt a proposal to address illicit trade in cultural goods to extend the scope of the current legislation to additional third-countries. The Commission also envisages a proposal to give law enforcement and other public authorities access to bank account registers. Moreover, the Commission recently adopted a report on the assessment of supranational risk of money laundering and terrorist financing[32], as well as a staff working document on improving cooperation between Financial Intelligence Units.[33] Later this year the Commission will report on its ongoing assessment of the need for possible additional measures to track terrorist financing in the EU. The Commission is also reviewing legislation on combatting fraud and counterfeiting of non-cash means of payments to take account of newer forms of crime and counterfeiting in financial instruments, with the aim to decrease its occurrence and deter potential criminal activities such as terrorist financing.

---

26 Council conclusions on the way forward to improve information exchange and ensure the interoperability of EU information systems: http://data.consilium.europa.eu/doc/document/ST-9448-2017-INIT/en/pdf.

27 Proposal for a **Directive to harmonise the definition and criminal sanctions of money laundering**, COM(2016) 826 final (21.12.2016).

28 Proposal for a **Regulation to uncover illicit cash payments**, COM(2016) 825 final (21.12.2016).

29 Proposal for a **Regulation on the mutual recognition of criminal asset freezing and confiscation orders**, COM(2016) 819 final (21.12.2016).

30 COM(2016) 450 final (5.7.2016).

31 See table in Annex 2 listing the action taken to implement the February 2016 Action Plan.

32 COM(2017) 340 final (26.6.2017).

33 SWD(2017) 275 (26.6.2017).

3. External dimension

The need to reinforce the **external dimension** of countering terrorist financing and money laundering is highlighted in the conclusions the Foreign Affairs Council adopted on 19 June 2017 on the external dimension of counter-terrorism.[34] The conclusions confirm the geographic and thematic priorities for future external counter-terrorism activity, namely strengthening counter-terrorism cooperation with priority third countries in the Middle East, North Africa, the Western Balkans and Turkey, as well as with strategic partners and international organisations. The conclusions have been strongly informed by the non-paper on external counter-terrorism action that the European External Action Service and the Commission presented in May 2017 to Member States.

On 16 June 2017, the **EU-U.S. Justice and Home Affairs Ministerial Meeting** took place in Malta, which was the first such meeting with the new U.S. Administration. The U.S. affirmed their wish to continue close cooperation with the EU and emphasised the need for swift information sharing in the fight against terrorism and organised crime. The Commission outlined the actions the EU is taking against Foreign Terrorist Fighters, with a focus on transatlantic information sharing. The EU and U.S. provided updates on actions against radicalisation online and offline, on developments regarding passenger name record (PNR) data, money laundering, border management and aviation security. On the question of risks to aviation security from personal electronic devices, the EU and U.S agreed to continue working together on raising global aviation security standards. The Commission updated Member States on the discussion and possible mitigating measures at the Committee for Civil Aviation Security on 21 June 2017, and will continue working closely with the U.S. at technical and political level to address developing threats.

V. CONCLUSION

This report focusses of the actions taken in the past months towards building an effective and genuine Security Union. The increase of terrorist attacks in recent weeks and months are another reminder of the importance of this work and the need to accelerate delivery. The actions outlined in this report require urgent implementation to counter the heightened threat of terrorism, to strengthen cooperation at EU level to prevent and counter radicalisation, to cut off the financing of terrorism and to step up the exchange of information and achieve the interoperability of information systems to close information gaps. The European Council conclusions of 22-23 June 2017 confirm the importance and urgency of this on-going work. The Commission calls on the European Parliament and the Council to continue and intensify these joint efforts to enhance the security of all citizens.

The next Security Union progress report in July 2017 will set out the results of the comprehensive assessment of the Union's action in the area of internal security and the conclusions the Commission draws from that inclusive consultation process launched in December 2016.

[34] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-conclusions-counterterrorism/.