EUROPEAN
COMMISSION

Brussels, 9.12.2020
COM(2020) 795 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond

I. INTRODUCTION

The European Union is a unique area of **freedom**, **security** and **justice**, where every person must be able to trust that their freedom and security are guaranteed and well protected. Democracy, rule of law, respect for fundamental rights in particular the right to privacy, freedom of expression, freedom of religion and the respect for diversity are the foundation of our Union.

The recent spate of attacks on European soil have served as a sharp reminder that terrorism remains a real and present danger. As this threat evolves, so too must our cooperation to counter it. The transnational nature of terrorist networks requires a strong collective approach at EU level, one that safeguards and upholds our **pluralistic society**, our **common values** and **our European way of life**. Citizens have the right to feel safe in their own homes and streets, as well as on the internet. The EU has a key role to play in helping to deliver that security.

This is all the more acute given that **the EU remains on high terrorist alert**. The jihadist threat from or inspired by Daesh, al-Qaeda and their affiliates persists[1]. Threats from violent right and left-wing extremists are on the rise. The nature of attacks is also shifting. The vast majority of recent attacks were carried out by individuals acting alone – often with limited preparation and easily available weaponry – targeting densely crowded or highly symbolic spaces. While single actor attacks are likely to remain prevalent, more sophisticated attacks cannot be excluded. The EU also needs to be prepared for threats from new and emerging technologies, such as malicious use of drones, artificial intelligence and chemical, biological, radiological and nuclear material. The spread of radical ideologies and of terrorist guidance material accelerates through the use of online propaganda, with the use of social media often becoming an integral part of the attack itself.

Over the last two decades, **European cooperation on counter-terrorism** has advanced steadily and enhanced the capacity of Member States to ensure the security of their citizens. We have extensive information-sharing networks, supported by increasingly interoperable EU databases as well as enhanced police and judicial cooperation. This helps us connect the dots across borders. We have also equipped ourselves with powerful tools to deny terrorists the means to act, such as in the areas of firearms, explosives precursors, terrorism financing and criminalising travel for terrorist purposes. The state of play of these efforts is set out in the **Security Union progress report**[2]. However, we need to redouble our collective work, in particular to counter the draw of extremist ideologies and better protect the public spaces targeted by terrorists. We must also overcome the false dichotomy between online and off, bringing the respective security environments in line, and equipping law enforcement and judicial authorities with the means to enforce the law in both.

This new **Counter-Terrorism Agenda,** announced in the EU's Security Union Strategy[3], brings together existing and new strands of work in a joined-up approach to combatting terrorism. This approach will be brought forward in coordination with the Member States, while working with the European Parliament and the Council[4], and also by engaging society as a whole: citizens, communities, faith groups, civil society, researchers, businesses and private partners. The Agenda builds on what has been achieved over the past years and sets

1 See EEAS(2020) 1114.
2 COM(2020) 797.
3 Commission Communication on the EU Security Union Strategy, 24.7.2020, COM(2020) 605 final.
4 Cf. most recently the videoconference of Home Affairs ministers of 13 November 2020 which adopted a joint statement: https://www.consilium.europa.eu/en/meetings/jha/2020/11/13/

out a series of actions to be taken forward at national, EU and international level across four fronts:

Firstly, we need to be able to better **anticipate** existing and emerging threats in Europe. Information sharing and a culture of cooperation that is multi-disciplinary and multi-level remain key for a solid threat assessment that can form the basis of a future-proof counter-terrorism policy.

Second, we need to work to **prevent** attacks from occurring, by addressing and better countering radicalisation and extremist ideologies before they take root, making clear that respect for the European way of life, its democratic values and all it represents is not optional. This Agenda sets out ways of supporting local actors and building more resilient communities as a matter of priority, in close coordination with Member States, taking into account that some attacks have also been carried out by Europeans, raised within our societies, who were radicalised without ever having visited a conflict zone.

Third, to effectively **protect** Europeans, we need to continue to reduce vulnerabilities, be it in public spaces or for the critical infrastructures that are essential for the functioning of our societies and economy. It is essential to modernise the management of the EU's external borders through new and upgraded large-scale EU information systems, with reinforced support by Frontex and eu-LISA, and ensure systematic checks at the EU's external borders. This is necessary to close what would otherwise be a security gap when it comes to returning foreign terrorist fighters.

Fourth, to **respond** to attacks when they do occur, we need to make the most of the operational support EU Agencies, such as Europol and Eurojust, can provide, as well as ensure we have the right legal framework to bring perpetrators to justice and to guarantee that victims get the support and protection they need.

Underpinning this approach is the need to continue to place a relentless emphasis on **implementation and enforcement**. To reap the benefits of EU-wide harmonisation and cooperation, it is of fundamental importance that there are no gaps or delays in how we apply key instruments, such as the Directive on combating terrorism[5], the Firearms Directive and legal framework on combating money laundering and terrorist financing[6].

Finally, **international engagement** across all four pillars of this Agenda, facilitating cooperation and promoting capacity building, is essential to improve security inside the EU.

II. A FOUR PILLAR STRATEGY TO COUNTER TERRORISM: ANTICIPATE, PREVENT, PROTECT AND RESPOND

1. ANTICIPATE

Anticipating blind spots remain key means of strengthening Europe's counter-terrorism response and staying ahead of the curve.

[5] Directive (EU) 2017/541 of 15 March 2017 on combating terrorism, OJ L 88/6, 31.3.2017.

[6] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, OJ L 284, 12.11.2018. Denmark and Ireland are not bound by the Directive. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156/43, 19.6.2018.

Strategic intelligence and threat assessment

Strategic intelligence is of key importance to shape and develop an increasingly threat-based EU counter-terrorism policy and legislation, and better anticipate those threats. Future-proof counter-terrorism policy should be based on solid threat assessments in particular from **national security and intelligence services**. In this context, the role played by the EU Intelligence and Situation Centre (EU INTCEN) and its expertise on the main threats, trends and modus operandi related to EU internal security is vital to increase our situational awareness and support our risk assessment capability. EU INTCEN critically depends on high quality input from Member States, which they should strive to improve. Member States should therefore ensure that EU INTCEN can rely on accurate and up-to-date input and sufficient resources. The Commission and the EEAS will strive towards better integrating strategic intelligence in counter-terrorism policies. Further dialogue, building upon existing structures and building on the work of the EU Counter-terrorism Coordinator to enhance the cooperation is of key importance.

Risk assessments and preparedness

Targeted risk assessments allow stakeholders of different sectors to highlight existing shortcomings and therefore better anticipate possible attacks. The Commission will propose new ways to encourage risk assessment and peer review activities of measures aimed at better anticipating the terrorist threat. As part of the upcoming proposal on the **resilience of critical entities**, the Commission will propose to set up advisory missions to support host Member States and operators of critical infrastructures of particular European significance in enhancing their resilience to disruptions, including anticipating possible terrorist actions. This will build upon the experience of a pool of protective security advisors, who are currently being trained, and who can be deployed on demand: the **EU Protective Security Advisory missions.**

EU aviation security risk assessments will be further developed in order to enhance both the response time after incidents and the level of exchange of information, including the participation of like-minded third countries, notably the U.S., Australia and Canada. The Commission will also launch a new risk assessment strand to ensure the **security of transport in the maritime area**. Lastly, joint training and exercises will play an important part in the efforts to strengthen the preparedness and resilience of Member States, the EU institutions and bodies, as well as international partners[7].

Reinforcing early detection capacity

The crucial role that modern technology can play in committing terror was illustrated by the extreme right-wing terrorist attack on a synagogue in Halle, Germany, in 2019, where the attacker constructed several guns using 3D printing. We need to better anticipate how technologies impact the terrorist threat in order to equip law enforcement authorities with the right tools.

EU security research will focus on addressing different modi operandi, building on initiatives intended to enhance the capacity of law enforcement authorities as regards

[7] In the framework of the pilot project for Parallel and Coordinated Exercises (PACE) agreed with NATO, two sets of exercises have already been organised in 2017 and 2018. Efforts are currently focused on implementing the lessons identified during those exercises. The EU and NATO have agreed to extend the PACE concept for the period 2022-2023. As a long-term objective, the EU supports a more ambitious approach on PACE exercises, including the active participation of EU Member States and NATO allies in their conduct phase.

analytical solutions and dealing with large amounts of online content[8]. EU-funded security research will also strengthen the **early detection capacity** of potential terrorist threats, notably by exploring the use of Artificial Intelligence to allow for more efficient and accurate processing of large amounts of data, adding on projects like RED-Alert[9] and PREVISION[10]. It can also help to find new ways to address radicalisation.

Lastly, under the future **Research Programme Horizon Europe**, research will be further integrated within the security policy cycle to ensure an even more impact-oriented output, responding to the identified law enforcement needs. With its proposed strengthened mandate, Europol could assist the Commission in identifying key research themes, drawing up and implementing the EU framework programmes for **research and innovation** that are relevant for law enforcement.

Staying ahead of the curve: the role of new technologies

Threat **detection technologies** can detect objects and substances of concern, for example bombs or bomb-making materials. The Commission is working together with the private sector to **improve the performance** of such detection technologies outside aviation[11] with a view to support the possible development of voluntary EU requirements for detection technologies to ensure that they detect the threats they need to detect while preserving the mobility of people. In addition, in 2019, the **EU Rail Security Platform** adopted a good practices' document on security technologies adapted to railways, proposing solutions such as random or targeted checks relying on mobile detection equipment.

New technologies can contribute to the protection of public spaces if they are used in a well-defined, targeted and proportionate manner. In case of high terrorist threat alert[12], the possible role of facial identification technologies capable of detecting terrorists on the move by comparing their facial image with a reference database holds security potential. Moreover, identification of certain categories of objects (e.g. abandoned luggage) or suspicious behaviour can be highly useful to detect threats. Artificial Intelligence plays a key role in delivering tools that allow for precise and targeted identification of potential threats. In the reflections that the Commission is undertaking on the use of Artificial Intelligence,[13] security considerations will therefore be taken into account, subject to compliance with fundamental rights. The Commission is ready to **fund projects to develop new technologies** under the Urban Agenda for the EU, and supports the exchange of best practices in this area in

8 Following up on successful initiatives such as projects DANTE and TENSOR. The DANTE project has delivered effective, efficient, automated data mining and analytics solutions and an integrated system to detect, retrieve, collect and analyse huge amounts of heterogeneous and complex multimedia and multi-language terrorist-related contents, from the surface, deep web and dark nets. (https://cordis.europa.eu/project/id/700367). TENSOR has had an approach complementary to DANTE and developed a platform that provides police authorities with tools necessary to enhance their capacity for dealing with huge amounts of online content in the early detection of online terrorist organised activities, radicalisation and recruitment. (https://cordis.europa.eu/project/id/700024)

9 RED-Alert uses advanced analytics techniques, such as natural language social network analysis, artificial intelligence and complex event processing, to tackle law enforcement needs in terms of prevention and action regarding terrorist social media online activity. (https://cordis.europa.eu/project/id/740688)

10 PREVISION is an on-going project the objectives of which are to provide law enforcement with the capabilities of analysing and jointly exploiting multiple massive data streams, semantically integrating them into dynamic knowledge graphs as well as predicting abnormal or deviant behaviour and radicalisation risks. (https://cordis.europa.eu/project/id/833115)

11 In the area of civil aviation, a legal framework sets out performance standards for detection equipment. This framework only applies to aviation security and not, for example, for detection equipment used to protect other public spaces.

12 Terrorist alert level as defined by national authorities, in line with their national law.

13 White Paper on Artificial Intelligence: A European approach to excellence and trust (COM(2020) 65 final, 19.2.2020).

accordance with EU law.

Developments in **Artificial Intelligence** (AI) are set to have a profound impact on the ability of law enforcement authorities to respond to terrorist threats. Law enforcement authorities are already developing **innovative solutions** based on AI technology, for example to identify terrorist content online and stop its dissemination, to prevent the creation of new terrorists' accounts on social media, and detect symbols. One key aspect to developing trustworthy AI applications is ensuring that the data used to train algorithms is relevant, verifiable, of good quality and available in high variety to minimise bias for instance towards gender or race. AI applications should be developed and used with proper safeguards for right and freedoms, in compliance with relevant legislation and adequately documented to ascertain the legality of their use. The Commission will look into how law enforcement and judicial authorities may harvest the benefits of AI in full conformity with EU law.

Staying ahead of the curve also means addressing emerging threats that may be posed by new technologies. **Drones** (Unmanned aircraft systems) can be misused to target public spaces, individuals and critical infrastructure. While the EU has made it more difficult to use certain types of drones for malicious purposes[14], the rapid pace of innovation and easy access to drones means that the threat is likely to grow. To confront this challenge, the Commission will look into the possibility of releasing in 2021 an **EU handbook for securing cities** from non-cooperative drones.

Protecting from malicious drones also requires access to reliable counter-measure technologies. The "European Programme for counter-UAS systems testing" will create a common methodology to evaluate different systems that can be used by police and other security actors to **detect, track and identify** potentially malicious drones. The outcomes of these tests will be shared EU-wide.

Integrating foresight in the policy cycle

Protecting citizens starts with a better understanding of future threats. To that end, foresight needs to be structurally integrated in the development of counter-terrorism policy. The Commission will work towards creating a dialogue between senior counter-terrorism experts from law enforcement, intelligence and academia on a regular basis to identify new risks and highlight areas where the European Union and its Member States need to bolster their action. The Commission will use existing structures for this purpose with the close involvement of Europol, Eurojust, and the EEAS including EU INTCEN[15]. The result of this dialogue could then feed into policy discussions, including the Justice and Home Affairs Council discussions on internal security.

[14] Through the new European drone regulations and the prospect of a European unmanned traffic management framework (the U-Space). Recent EU legislation in this area will contribute to the security of drone operations by requiring most drones to be equipped with remote identification and geo-awareness functions. From January 2021, drone operators will also be required to register with national authorities. This is complemented by a proposal from the Commission on a **regulatory framework for the U-space**, Europe's unmanned traffic management system[14], to ensure the safe and secure operations of drones.

[15] Cf. Council Conclusions on EU External Action on Counter-terrorism of 19 June 2017.

KEY ACTIONS

The Commission will:

- Develop risk assessment and peer review activities, including the on-demand deployment of EU Protective Security Advisors.
- Fund EU-security research to strengthen early detection capacity and develop new technologies under the Urban Agenda for the EU.
- Explore how new technologies can contribute to security. Better integrate strategic intelligence and threat assessments to support forward looking policy.

Member States are urged to:

- Continue providing EU INTCEN with necessary resources and high quality input.

2. PREVENT

The European Union is founded on a strong set of values. Our education, health and welfare systems are inclusive by nature but they come part and parcel with acceptance of the values that underpin them. Our European way of life – emblematic of inclusive and tolerant societies – is not optional and we must do all in our power to prevent those that seek to undermine it – from within or without.

Countering extremist ideologies online

Terrorists and violent extremists increasingly make use of the internet to disseminate their extremist ideologies, including by live streaming and glorifying terrorist attacks. The response must come from all actors – national authorities, industry and civil society – and at all levels (national, European and international). The adoption and implementation of the proposed **Regulation on addressing the dissemination of terrorist content online** would allow Member States to ensure the swift removal of such content and require companies to be more responsive in preventing the abuse of their platforms for the dissemination of terrorist content. Adoption by the European Parliament and the Council is therefore a matter of urgency. Once adopted, the Commission will support online service providers and national authorities in the effective application of the Regulation.

More broadly, the Commission will propose a **Digital Services Act** which will upgrade the horizontal rules to ensure digital services act responsibly and that users have effective means to notify illegal content. Recognising the increasing societal role of very large online platforms, the proposal will include obligations to assess the risks their systems pose not only as regards illegal content and products, but also systemic risks to the protection of public interests, such as public health and public security, and fundamental rights, also against manipulative techniques.

The **EU Internet Forum** will develop guidance on moderation for publicly available content for extremist material online and further disseminate knowledge in that area. The EU Internet Forum developed the **EU Crisis Response Protocol**, a voluntary mechanism to help coordinate a rapid, collective and cross-border response to the viral spread of terrorist and

violent extremist content online[16]. It is essential that industry partners fully operationalise this protocol. The Commission, in cooperation with Europol, will support the development of further guidance for the implementation of the EU Crisis Protocol to tackle a viral spread of terrorist and violent extremist content online. **Europol's Internet Referral Unit's** resources and capacity should be reinforced to monitor and refer all types of terrorist content to online platforms with a 24/7 availability.

Terrorist content originates and spreads from all over the world. This is why the Commission will increase its engagement with **international partners,** in particular with the **Global Internet Forum to Counter Terrorism (GIFCT)** for a global operational response, as well as with partner governments, in line with the **Christchurch Call for Action**[17] to strive towards minimum standards globally, including on transparency.

To respond to the proliferation of racist and xenophobic hate speech on the internet, the Commission encouraged the signing of the **EU Code of Conduct on countering illegal hate speech online** in 2016[18]. The Commission will present an initiative in 2021 to extend the list of EU-level crimes under Article 83(1) of the Treaty on the Functioning of the EU to hate crime and hate speech, whether based on race, ethnicity, religion, gender or sexuality. Member States should step up their efforts to fully implement the new Audio-visual Media Services Directive provisions on hate speech on online video-sharing platforms.

The Commission will support Member States to develop their **strategic communication** capabilities for post-attack responses through exchange of expertise at local and national level. This is necessary not only in the aftermath of a terrorist attack, but it should be an ongoing governmental preventive effort. The Commission will therefore support Member States to address these challenges and increase the dissemination of counter- and alternative narratives developed by civil society and support similar efforts at national level. The Commission's **Civil Society Empowerment Programme** will be evaluated in 2022 to provide lessons learnt.

At the same time, both the EU and its Member States must continuously ensure that projects which are incompatible with European values or pursue an illegal agenda, do not receive support from **government and European funds**.

Supporting local actors for more resilient communities

Our cities need to have better access to funding, guidance and training to address current challenges and to increase their resilience. The Commission is supporting local prevent coordinators through the **Radicalisation Awareness Network**. Furthermore, under the initiative "EU Cities against Radicalisation", the Commission is fostering strategic dialogues among cities. To increase resilience, it is also important to **engage with communities** and empower them through a bottom-up approach, in close coordination with Member States. The

[16] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20191007_agenda-security-factsheet-eu-crisis-protocol_en.pdf

[17] https://www.christchurchcall.com/call.html

[18] The results are overall positive with IT companies assessing 90% of flagged content within 24 hours and removing 71% of the content deemed to be illegal hate speech. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

Radicalisation Awareness Network will identify best practices and foster approaches of community policing[19] and engagement to build trust with and among communities.

Promoting inclusion and providing opportunities for young people at risk through education, culture, youth and sports can further contribute to the prevention of radicalisation, and cohesion inside the EU. The Commission will reinforce its support to Member States and other stakeholders' efforts in the field of **integration and social inclusion** through the measures included in the Action Plan on integration and inclusion[20].

Given the important **role of non-formal education** in radicalisation and possible links to extremist ideologies, the Commission will facilitate collaboration among **schools, communities (including faith groups), youth workers, social workers and civil society organisations**. The Commission will also support Member States in sharing experiences and good practices with regard to exchanges among religious and community leaders on the prevention of radicalisation, including those active in schools and prisons.

Real or perceived social exclusion, discrimination and marginalisation can reinforce vulnerability to radical discourses and further threaten social cohesion. The Commission will therefore also continue its action set out in its anti-racism action plan.[21]

Prisons, rehabilitation and reintegration

Radicalisation processes need to be spotted as early as possible so that disengagement activities can be implemented timely. We will strengthen EU action on three key areas: **prisons, rehabilitation and reintegration**. First, by identifying best approaches regarding management and risk assessment of radicalised inmates and terrorist offenders[22], as well as supporting training of professionals involved in this field[23]. Second, by building on the insights of the Radicalisation Awareness Network Rehabilitation Manual,[24] the Commission will support Member States to provide more tailored guidance on rehabilitation and reintegration of radical inmates, including after release. Thirdly, by developing a methodology with common standards and indicators for evaluating the effectiveness of reintegration programmes[25]. Any efforts with regard to rehabilitation and reintegration of children need to take into account their specific needs and rights[26].

Foreign terrorist fighters and their family members, including those currently located in detention centres and camps in North East Syria, raise specific and complex challenges, which require coordination of stakeholders at all levels. The Commission will further support

---

19 In this context, community policing is a collaborative effort between law enforcement and communities to prevent and counter challenges related to violent radicalisation.

20 COM(2020) 758 final.

21 A Union of equality: EU anti-racism action plan 2020-2025 (COM(2020) 565 final, 18.9.2020).

22 The Commission will also work on the issue of pre-trial detention, keeping in mind that long periods of pre-trial detention may enhance the risk of radicalisation.

23 This includes prison and probation staff, as well as other professionals working in prisons and after release (e.g. chaplains, psychologists, social workers, NGOs, etc.).

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

25 Responses on collaboration models and protocols for disengagement and reintegration, as well as preparedness of stakeholders will be provided by projects under a dedicated Internal Security Fund call of 4 MIO EUR. The projects will address disengagement and reintegration of extremist offenders and radicalised individuals related to violent right wing and Islamist extremism, including returning foreign terrorist fighters and their families.

26 Directive (EU) 2016/800 on procedural safeguards for children who are suspects or accused persons in criminal proceedings, OJ L 132/1 of 21.5.2016. See Recital 9: "Children who are suspects or accused persons in criminal proceedings should be given particular attention in order to preserve their potential for development and reintegration into society.

Member States to share best practices and will also increase support to the training of practitioners, and to knowledge and information sharing in this area, taking into account the specific needs and rights of children of foreign terrorist fighters. In addition, the Commission will also support Member States to step up efforts towards ensuring the prosecution of foreign terrorist fighters by supporting work to that end at local, national and international.

Consolidating knowledge and support

For more coordinated action and structured outreach at national level, in a first phase the Commission will support the creation and further development of **national networks** of relevant actors, including practitioners and **national centres of expertise**[27]. In a second phase, the Commission will propose setting up an **EU Knowledge Hub on prevention of radicalisation** for policy makers, practitioners and researchers. The EU Knowledge Hub would disseminate knowledge and expertise and also promote the full use of **funding possibilities under the various EU programmes**[28], evaluate interventions, certify best practices and offer targeted support to stakeholders at national and local level. It could also possibly integrate a future EU centre for victims of terrorism to offer expertise and support to national authorities and victims support organisations[29]. Other relevant areas include research, provision of information about radical ideologies, organisations and networks and the dissemination of counter- and alternative narratives, as well as cooperation with community and religious leaders.

Finally, building on research, the Commission will develop guidance for Member States and other stakeholders regarding **lone actors** including risk assessments and possible responses to this phenomenon.

[27] Possibly co-financed through the national programmes of the Internal Security Fund.

[28] In particular the funding under the Internal Security Fund, the Citizenship, Equality, Rights and Values Programme, the Justice Programme, the European Regional Development Fund, the European Social Fund Plus and Erasmus+.

[29] Such a future Centre could build on the work of the two-year pilot project EU Centre of Expertise for victims of terrorism and ensure close cooperation with existing networks in the area of victims' rights such as the European Network on Victims' Rights and the Single contact points for victims of terrorism.

KEY ACTIONS

The Commission will:

- Propose a Digital Services Act.
- In cooperation with Europol, provide guidance for the implementation of the EU Crisis Protocol
- Support Member States to develop strategic communication and increase the dissemination of counter- and alternative narratives.
- Provide guidance on management and risk assessments in prison and on early rehabilitation and reintegration.
- Foster best practices sharing between Member States to manage returning foreign terrorist fighters and their family members.
- Propose setting up an EU Knowledge Hub on the prevention of radicalisation and support national networks of stakeholders and national centres.

The European Parliament and the Council are urged to:

- Adopt, as a matter of urgency, the Regulation addressing the dissemination of terrorist content online.

The Commission and the Member States will:

- Ensure that projects which are incompatible with European values or pursue an illegal agenda do not receive support from public funds. Build community resilience through the measures included in the Action Plan on integration and inclusion.

3. PROTECT

Strengthening the counter-terrorism response must include reducing vulnerabilities that can be exploited or targeted by terrorists. By better protecting our borders and denying terrorists the means used to carry out terrorist acts, we can protect against potential attacks.

Protecting people in public spaces

Terrorist attacks have overwhelmingly targeted people in public spaces, which are especially vulnerable due to their open and accessible nature. We need to safeguard the open nature of these spaces while at the same time making them more secure through stronger **physical protection** measures that do not create fortresses[30] and still allow people to walk about freely and safely. This is why the Commission will increase efforts at EU level to promote **security-by-design** solutions, which build security into public spaces (buildings and infrastructures) from the beginning of the design and urban planning processes. The Commission will issue a virtual **architectural book on urban design**, which can serve as inspiration for authorities to incorporate security aspects in the design of future and the renovation of existing public spaces.

[30] The Commission has issued guidance material how to physically protect public spaces, e.g. https://ec.europa.eu/jrc/en/publication/guideline-building-perimeter-protection

The **EU Forum on the protection of public spaces** has brought together a wide group of people with responsibility over the security of public spaces. These include EU Member States' authorities, and private operators, e.g. those responsible for shopping malls, transport services, or venues for hospitality. There is much to be learned from different experiences in protecting public spaces[31]. The Commission is committed to enhancing this forum, which should collect, consolidate and disseminate knowledge, as well as support the EU Pledge on Urban Security and Resilience, and to use targeted funding to help improving the protection of public spaces[32]. The Commission will also explore the possibility of **setting minimum obligations** for those that are responsible for guaranteeing the security of public spaces to clarify what can be expected from the operators of public spaces.

Places of worship hold a particularly high symbolic value and have frequently been targeted by terrorists. We must better protect churches, mosques and synagogues as well as other religious sites across the EU. We should also foster cooperation between the different faith communities and the relevant national authorities as they exchange experiences. As from 2021, the Commission aims to support projects that enhance the physical protection of places of worship in close coordination with Member States.

Cities as the backbone of urban security

Local and regional authorities play a key role both in the protection of public spaces and the prevention of radicalisation. In cooperation with the Urban Agenda for the EU Partnership for Security in Public Spaces and building on the successful initiative EU Cities against Radicalisation, the Commission will propose an **EU Pledge on Urban Security and Resilience**, setting out basic principles and objectives for local authorities in these areas, and will call upon interested cities to sign up to a positive agenda to prevent and counter radicalisation and reduce vulnerabilities in public spaces. Cities which take part in the Pledge will become part of an EU-wide initiative of **Cities against Radicalisation and Terrorism**, through which the Commission will facilitate the sharing of good practices and support projects led by cities and peer-to-peer advisory efforts. The Commission will mobilise all available funding instruments to support the implementation of the Pledge.

In addition to the Internal Security Fund, EU Cohesion policy funds can be used for increasing public security in cities through investments aimed at enhancing their social cohesion, integration and resilience to prevent radicalisation and upgrade public infrastructure. The Commission will work with Member States to increase the awareness regarding the available funding opportunities and calls upon Member States to make full use of the EU Cohesion policy funds to include such investments in their post-2020 programmes. The investments derived from integrated sustainable urban development strategies will account, as proposed by the Commission, for more than 6% of the European Regional Development Fund allocation.

Making critical infrastructure more resilient

Critical infrastructure, including transport hubs, power stations, health care infrastructures

[31] See also Commission Staff Working Document – Good practices to support the protection of public spaces, 20.3.2019, SWD (2019) 140 final.

[32] Under the Internal Security Fund – Police, the Commission has issued calls for projects that improve the protection of public spaces in 2017, 2019, and 2020 worth over 40 million EUR to stakeholder-led initiatives. The Fund has also supported the trainings and exercises of various law enforcement networks that protect public spaces against terrorism, such as the ATLAS network of special interventions unit, and the launch of the Protective Security Advisory activities.

and water treatment facilities, run the risk of being potential terrorist targets. Critical infrastructure operators are responsible for providing services that are essential in meeting vital societal needs. At the same time, these operators continue to grow increasingly dependent on one another and face an ever more complex risk environment. Such risks include terror attacks, natural disasters, accidents, and malicious threats. In order to ensure the dependable provision of essential services across the EU and the reliable functioning of the internal market, it is vital to ensure that critical operators of essential services are resilient, i.e. sufficiently prepared to prevent, mitigate, and recover from disruptions. The Commission will adopt a **set of measures** aimed at enhancing the resilience of operators in the face of both physical and digital risks.

Border security

Foreign terrorist fighters who had returned clandestinely from Syria were involved in the deadly attack in Paris on 13 November 2015. This highlighted the devastating consequences of failures in border security[33]. It is estimated that 50 000 persons have travelled to Syria and Iraq to join jihadist groups, including 5 000 individuals from the EU, of which around one third are still located in the area. To guarantee the security of our citizens, it is of crucial importance that law enforcement authorities can detect both EU and non-EU citizens suspected of terrorism at the external borders. Europol, Frontex and eu-Lisa will continue to support Member States on border security.

It is necessary to strengthen the functioning of the Schengen area without internal borders. On 30 November 2020, the Commission held a Schengen Forum to launch an inclusive political debate towards building a stronger Schengen based on mutual trust. This will feed into the Schengen Strategy which the Commission plans to present in 2021, and where it will propose ways to review the Schengen Borders Code, to improve the mechanism of evaluation and enhance the Schengen governance, to enhance police cooperation and information exchange and reinforce the external borders.

At the same time, Member States should urgently complete the modernisation of external border management within the agreed roadmaps, with the ambition of developing the most modern border management system[34]. Despite the progress made, more work is needed. While Member States may apply derogations under certain conditions, it is important that they rapidly meet the objective of **systematic checks of all travellers against relevant databases** at the external borders. In mid-2021, the Commission will prepare **guidance**, in collaboration with Member States, to ensure that any derogations are used in a limited manner and meet the highest security standards.

The effectiveness of systematic checks depends on the quality and **interoperability of EU information systems**[35]. New and upgraded large-scale EU information systems[36] will

---

[33] Perpetrators of the November Paris attacks were members of IS in Syria or Iraq. [...] In previous years it had been reported that the majority of FTFs use their own genuine documents to travel. However, use of false documentation clearly does occur, as was the case with a number of individuals involved in the November Paris attacks (Europol, European Union Terrorism Situation and Trend Report, 2016).

[34] Implementation of the new IT-architecture and interoperability, implementation of EBCG 2.0, swift adoption of the Screening proposal.

[35] https://www.eulisa.europa.eu/Activities/Interoperability. In accordance with the European Interoperability Framework: https://ec.europa.eu/isa2/eif_en ; See COM(2017)134 final.

[36] The Schengen Information System, the Entry/Exit System, the Visa Information System, Eurodac, the European Criminal Records Information System (its part related to third country nationals and stateless persons).

improve security and make external border controls more effective and efficient. Interoperability will make the necessary information instantly available to those police officers and border guards with a need to know. Of crucial importance is the **Entry/Exit System** (EES)[37], which is an automated system for registering travelers from third countries. This will help identify all third-country nationals entering the territory of Member States and detect identity fraud.

The European Travel Information and Authorisation System (ETIAS)[38], a pre-travel authorisation system for visa-exempt travelers, is equally important. A dedicated **ETIAS watchlist** will enable better use of information on persons suspected of or linked to terrorist activities, allowing Member States to consider that information when issuing authorisations to travel. Additionally, the checks against the future centralised system for the identification of Member States holding conviction information on third-country nationals and stateless person (**ECRIS-TCN)**[39] will allow for verification whether a certain third-country national or dual EU/third-country national had been previously convicted of serious crime in the EU and in which Member State. Interoperability between EES, ETIAS and ECRIS-TCN will lead to more systematic information for law enforcement officers, border guards and migration officials, and will contribute to fighting identity fraud. Member States should therefore swiftly and completely implement these systems and allow for their interoperability.

The three new **Schengen Information System (SIS)** Regulations that entered into force in December 2018[40], introduced a number of measures to improve the information exchange including on terrorist suspects. It is crucial that Member States implement all **new SIS functionalities** as soon as possible. In particular, Member States should urgently roll out **the fingerprint search functionality** in the SIS Automated Fingerprint Identification System (AFIS) to their officers, in particular at the external borders.

It is also essential that **third-country information on foreign terrorist fighters**, provided by trusted third countries, is entered into SIS. Together with this Communication, the Commission is presenting a strengthened Europol mandate and an amendment to the Regulation on the establishment, operation and use of the Schengen Information System (SIS) that would allow-Europol to create dedicated alerts in SIS, in consultation with Member States. It is urgent that the voluntary procedure to process pending and future data provided by third countries discussed among Member States is put in place. In parallel, Member States should be encouraged to make Interpol's notices related to terrorist suspects available at the first line border checks.

Moreover, under the new rules, in addition to issuing **entry bans**, of up to 5 years, as part of a return decision[41], Member States should enter **alerts in SIS** on third-country nationals subject to a return decision (as of 2022), and on refusals of entry and stay. This would make return decisions and the prohibitions of entry and stay visible to all authorities having access to SIS. Member States should ensure that such alerts also contain information concerning the

[37] As established by Regulation (EU) 2017/2226, 9.12.2017, OJ L 327.
[38] As established by Regulation (EU) 2018/1240, 19.9.2018, OJ L 236/1.
[39] As established by Regulation (EU) 2019/816, 22.5.2019, OJ L 135/1.
[40] Regulation (EU) 2018/1860, Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862.
[41] Directive 2008/115/EC. The length of an entry ban may exceed 5 years if the third-country national concerned represents a serious threat to public policy, public security or national security. In addition, Member States remain free to adopt measures to prohibit entry into and stay against third-country nationals staying in a third country.

fact that the third-country national poses a serious threat to security, and whether the person was involved in terrorism-related activities.

The processing of **Advance Passenger Information (API) and Passenger Name Record (PNR)** data plays a vital role in identifying, preventing, detecting, and disrupting terrorism and other serious crimes. With a view to streamlining the use of API data, including for countering terrorism, the Commission will make a proposal to **revise the API Directive** in 2021 and consider providing for the use of this data for countering serious crime, improve the effectiveness in the use of API data and the coherence with other instruments such as the Entry/Exit System, the European Travel Information and Authorisation System, and the PNR system.

The **use and analysis of PNR data** is an essential tool to fight terrorism and organised crime, both in the EU and globally. The analysis of retained PNR data enables identification of previously unknown threats and provides law enforcement authorities with criminal intelligence leads, allowing them to detect suspicious travel patterns and identify associates of terrorists and criminals. The Commission urges Member States that do not do so already to also collect PNR Data for intra-EU flights. The Commission will continue to engage in the process of facilitating transfers of PNR data in full compatibility with EU legal requirements as clarified by the Court in the framework of the new PNR standards adopted by the International Civil Aviation Organisation (ICAO). The full implementation of the current PNR framework and the existing bilateral cooperation with third countries, such as the U.S. and Australia, remain key. At the same time, global trends and new realities[42] have emerged since 2010, when the Commission last updated its external PNR policy, which will be reflected in next year's **review of the EU external strategy towards PNR transfers**.

In light of the terrorist threat to aviation, efforts need to continue to step up aviation security. The Commission will explore options to create and implement a European legal framework for the deployment of security officers to be present on flights (air-marshals).

Denying terrorists the means to attack

In order to close an existing loophole, the Commission will adopt an **implementing regulation** under the Firearms Directive, establishing **a system for exchange of information** amongst Member States on refusals to grant authorisations for acquiring a firearm. This will ensure that a person who has been denied a firearm on security grounds in one Member State, cannot lodge a similar request in another Member State. This work is complemented by the **EU action plan on firearms trafficking**.[43] National Firearms Focal Points are essential to developing a genuine knowledge of the firearms-related threat by ensuring cross-departmental cooperation and cross-border[44] exchanges of information and intelligence. Within the "firearms" priority of the European Multidisciplinary Platform Against Criminal Threats (EMPACT), in 2021 the Commission will publish a scoreboard displaying how advanced Member States are with establishing such focal points.

---

42 Such as the existence of the PNR Directive and EU data protection instruments.

43 COM(2020) 608.

44 "cross-border" means "across any border", while also specifically meaning "issues impacting specifically on regions on both sides of a shared internal or external border".

The threat from **homemade explosives** remains high, as exemplified by multiple attacks throughout the EU[45]. The EU has developed the most advanced legislation in the world to restrict access to **explosives precursors**[46] and detect suspicious transactions that could lead to terrorists building homemade explosives. It is therefore crucial that Member States fully implement and enforce the new rules, which will come into effect on 1 February 2021. This includes ensuring that people cannot by-pass controls by buying explosives precursors online.

The risk from **chemical, biological, radiological and nuclear** (CBRN) materials remains a concern[47]. In 2017, terrorists plotted to detonate a bomb on an Australian plane and to build a chemical weapon, following instructions from Daesh[48]. In 2018, a terrorist attempted to create the highly poisonous ricin toxin in Germany[49]. The potential damage of a CBRN attack is extremely high. The Commission prioritises in particular the threat from **chemical agents**. Taking inspiration from the approach used to regulate access to explosives precursors, the Commission is studying the feasibility of restricting access to certain dangerous chemicals, to be finalised in 2021. In 2020, the Commission made available various instruments[50] to Member States that can be used to enhance **biosecurity**, and will explore how to improve cooperation against biological threats at EU level. Starting early 2021, the Commission is also supporting a joint action with 18 countries to strengthen health preparedness and response to biological and chemical terror attacks, and to strengthen cross-sectoral cooperation (health, security and civil protection).

Existing counter-terrorism restrictive measures ("sanctions") consist of a travel ban on natural persons and an assets freeze, and prohibition from making funds and economic resources available to natural persons and entities. The EU implements counter-terrorism sanctions adopted at UN level, and has adopted sanctions of its own to support the fight against terrorism[51]. As such, counter-terrorism sanctions are a powerful precautionary instrument to deny terrorists resources and mobility. The existing sanctions regimes available to the EU should therefore be used to their fullest extent, including through robust enforcement.

---

45 Some examples of such devastating attacks include attacks in Oslo (2011), Paris (2015), Brussels (2016), and Manchester (2017). An attack with a homemade explosive in Lyon (2019) wounded 13 people.

46 Chemicals that could be misused to manufacture homemade explosives. These are regulated in Regulation (EU) 2019/1148 2019 on the marketing and use of explosives precursors, which will apply as of 1 February 2021.

47 Europol reported that in 2019, the intention to carry out terrorist attacks using CBRN materials continued to appear on terrorist online forums and social media. Closed online forums were used to discuss possible modi operandi and share knowledge via handbooks, manuals, posters and infographics containing recipes to produce and disseminate various agents (Europol, European Union Terrorism Situation and Trend Report, 2020).

48 https://www.bbc.com/news/world-australia-49764450

49 https://www.dw.com/en/cologne-ricin-plot-bigger-than-initially-suspected/a-44319328

50 Such as the Biosecurity Resource Toolbox, the creation of which the Commission funded. It was made available to Member States on 19 October 2020 during a meeting of the CBRN Advisory Group.

51 Common Position 2001/931/CFSP and Council Regulation (EC) 2580/2001; Council Decision (CFSP) 2016/1693 and Council Regulation (EC) 881/2002 and Council Regulation (EU) 2016/1686.

KEY ACTIONS:

The Commission will:

- Propose a Schengen Strategy in 2021.
- Propose an EU Pledge on Urban Security and Resilience, to prevent and counter radicalisation and reduce vulnerabilities in public spaces.
- Help enhance the physical protection of places of worship, in close coordination with Member States.
- Propose measures to enhance the resilience of critical infrastructure.
- Propose to revise the Advance Passenger Information Directive.
- Establish an information exchange system on refusals to grant authorisations for firearms.
- Follow-up with Member States on the implementation of relevant legislation and take further steps in infringement proceedings, as appropriate

The Member States are urged to:

- Swiftly address gaps and shortcomings in implementation of relevant legislation.
- Ensure systematic checks of all travellers against relevant databases at the external borders.
- Issue alerts in SIS on suspected foreign terrorist fighters.
- Urgently roll out the fingerprint search functionality in the SIS Automated Fingerprint Identification System.
- Swiftly implement EES, ETIAS and ECRIS-TCN and allow for their interoperability.
- Strengthen chemical and bio-security.

4. RESPOND

After a terrorist attack has occurred, urgent action is needed to minimise its impact and allow for the swift investigation and prosecution of the perpetrators. No Member State can do it on its own. Cooperation is needed both at the European level and internationally.

Operational support: strengthening Europol

Europol and its European Counter-Terrorism Centre (ECTC) are key to EU action on counter-terrorism and its operational support has increased fivefold over recent years (from 127 operational cases supported in 2016 to 632 cases in 2019). The ECTC is now part of every major counter-terrorism investigation in the EU. As part of the legislative initiative to **strengthen the Europol mandate**, we need to enable Europol to **cooperate effectively with private parties**. Terrorists abuse cross-border services of companies to recruit followers, to plan and carry out attacks, and to disseminate propaganda inciting further attacks. Many companies want to share data, but may not know with whom as it may be unclear which Member States have jurisdiction to prosecute the specific crime. Europol is best placed to

close this gap and be a first contact to identify and transmit the relevant evidence to the authorities of the Member States concerned.

Europol must also be able to support national counter-terrorism investigations with the **analysis of large and complex datasets** ('big data'). This will build on the successful work of Europol with Task Force *Fraternité* to support French and Belgian authorities in the investigation of the November 2015 Paris attacks and the March 2016 Brussels attacks.[52] Strengthening Europol's role in **research and innovation** will help national authorities in using modern technologies to counter the threat of terrorism. Terrorists mask their identity, hide the content of their communications, and secretly transfer illicit goods and resources by exploiting new technologies. Therefore, we need to step up Europol's operational support on decryption in full respect of EU law.

Law enforcement cooperation

To enhance cross-border cooperation, the Commission will propose an **EU 'police cooperation code'** at the end of 2021. This will streamline the different EU instruments of operational law enforcement cooperation into a coherent and modern consolidated EU legal regime, thereby also facilitating cross-border cooperation in the fight against terrorism. This proposal will also take stock of existing Council guidelines and of the most advanced bilateral or multilateral agreements in force between Member States[53].

The Commission will continue to support the activities of various **law enforcement networks**. These activities include, for example, joint trainings and exercises, developing channels and capabilities for cross-border communication and operations, and improving the pooling of resources that can be mobilised during incidents. The Commission will continue supporting and ensuring the sustainability of the **ATLAS network of special intervention units** of the EU Member States, which aims to improve police response in cross-border counter-terrorism operations.

Within **Interreg cross-border cooperation programmes**, the European Regional Development Fund (ERDF) has supported cooperation between police and other security services in internal border regions. Under the 2021-2027 programming period, while such support may continue, the ERDF may also contribute to actions in the fields of border and migration management, such as for the economic and social integration of third-country nationals, including beneficiaries of international protection.

The Commission will also encourage cross-sectoral cooperation with other crucial first response actors, such as those deployed under the **Union Civil Protection Mechanism**, which can play a crucial role in response to major incidents with the capacity to overwhelm national capacities, such as terrorist attacks or chemical, biological, radiological or nuclear incidents.

Strengthening information exchange

---

[52] Task Force *Fraternité* analysed 19 terabytes of information to investigate further the international connections of the terrorists by analysing communication, financial, internet and forensic records. Europol's processing of large and complex data resulted in 799 intelligence leads.

[53] The proposal will be accompanied by an impact assessment and consultation of Member States, Schengen associated countries and relevant EU bodies.

In order to prevent, investigate and prosecute terrorist and other criminal offences, law enforcement authorities need access to the relevant information at the right time. The existing **Prüm Decisions**[54] have been instrumental in allowing Member States to exchange fingerprints, DNA and certain vehicle registration data. However, in light of technical, forensic, operational and data protection developments, the Prüm Decisions should be updated and could be further extended to better support Member States in their criminal and terrorist investigations. The Commission will propose in 2021 a revision of the Prüm Decisions to assess how they can be adapted to make them fit for the current and future operational needs of law enforcement authorities and to align those decisions with the EU data protection legal framework.

Justice and Home Affairs Agencies (such as Europol, Eurojust and Frontex) will need to strengthen their coordination in order to combat terrorism. Together with Member States, and given their respective responsibilities, connecting factors should be identified and solutions implemented in view of an efficient approach at the EU level. The Commission will make specific proposals to that effect, in particular to establish an efficient mechanism of information exchange in counter-terrorism cases, which should include a digital collaboration platform for Joint Investigation Teams, and step up the implementation of a hit/no-hit system between Europol and Eurojust to detect links between their data. The Commission is also proposing as part of the reinforced mandate of Europol to establishing a hit/no-system between Europol and the European Public Prosecutor's Office (EPPO). In addition, it remains an objective to extend the mandate of the European Public Prosecutor's Office to cross-border terrorist crimes.

The recent series of attacks have highlighted the importance of a reliable analysis of the threat posed by **persons regarded as terrorists or violent extremists**. The Commission supports the work set out recently by the Council[55]. There is a need for more regular strategic discussions on this pertinent topic, better mutual understanding and awareness of national concepts, as well as **facilitation of information exchange** when it comes to entering relevant information into the **EU's information systems**. The regular strategic exchange should include exchanges on practical tools, such as risk assessments, and their evaluation.

While increased information exchange among EU Member States is an absolute necessity, it is not always sufficient to effectively address global threats. This is why, international cooperation is a key component to an effective response to threats. Bilateral agreements with key partners play an important role in exchanging information, securing evidence and investigative leads from jurisdictions outside the EU. In that regard, **Interpol**, the international criminal police organisation, fulfils an important role. Despite the long-standing cooperation between the EU and Interpol, there are areas where cooperation should be established or reinforced. Interpol is a key partner on counter-terrorism, for example due to their expertise on foreign terrorist fighters. This includes, for instance, their work on the collection of battlefield information and the prevention of undetected border-crossings. Several EU bodies are faced with the operational need to have access to Interpol databases to perform their tasks. In order to enable such access in accordance with the requirements of EU legislation, the Commission is preparing the appropriate instruments to **negotiate a cooperation agreement between the EU and Interpol.**

---

[54] Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA.

[55] In the respective part of the Council Conclusions on Internal Security as adopted by the JHA Council on 4 December and the detailed Conclusions agreed by the Terrorism Working Party and endorsed by COSI on 19 November.

Supporting investigations and prosecution

Financial Intelligence Units have an essential role in detecting financing of terrorism as they receive suspicious transaction reports from a wide range of financial and non-financial institutions, which they analyse with other relevant information before disseminating the results of their analysis to law enforcement authorities or prosecutors. The Commission will consider how to improve their analytic capacity through the establishment of an **EU Coordination and Support Mechanism for Financial intelligence units**[56].

Financial investigations following the money trail and identifying previously unknown associates are crucial. New structures are needed to support financial investigators, to facilitate their cross-border work and reinforce the effectiveness of financial investigations in terrorism cases. The Commission proposes to establish a **network of counter-terrorism financial investigators.** Such a network would support the exchange of investigation techniques and experiences on financial investigations, taking into account the work done by national Financial Intelligence Units. It should involve Europol and its European Financial and Economic Crime Centre, cooperate with the Network of Asset Recovery Offices, and contribute to improve investigators' analysis, understanding of trends and emerging risks, and strengthen their capacity.

To investigate terrorist financing and wider terrorist networks, investigators need access to **bank account information**. The Commission has highlighted the need for Financial Intelligence Units and law enforcement to have swift cross-border access to national bank account information in other Member States[57]. This could be achieved by means of an interconnection of central bank account registries, which the Commission deems feasible[58]. This would also respond to the Council's call on the Commission to consider enhancing the legal framework to interconnect national centralised mechanisms[59]. In 2021, the Commission intends to propose legislation to achieve this interconnection and create **interconnected bank account registers.** The Commission will consider enabling access to such register by law enforcement authorities and asset recovery offices, subject to an impact assessment including on fundamental rights and in full respect of principles of proportionality[60]. This will enhance cross-border cooperation. In 2021, the Commission will also reassess the threats and vulnerabilities related to the foreign financing of terrorism and the collection and transfers of funds through **non-profit organisations**[61]**,** taking into account recent developments in this area.

The **Terrorist Finance Tracking Programme**[62] (TFTP) has generated significant intelligence that has helped investigate and detect terrorist plots and trace those behind them[63]. The EU-US TFTP Agreement on the exchange of financial information gives the US and EU law enforcement authorities a powerful tool in the fight against terrorism and has safeguards that ensure the protection of EU citizens' privacy. The next joint review of the

56 As suggested in the Anti-Money-laundering Action Plan of 7 May 2020, C(2020) 2800 final.
57 The Anti-Money-laundering Action Plan of 7 May 2020, C(2020) 2800 final.
58 COM(2019) 273 final.
59 June 2020 Council Conclusions on enhancing financial investigations, Council doc. 8927/20.
60 See also COM(2020)605 final.
61 Previous assessments were made in the Commission's 2019 Supranational Risk Assessment, COM(2019) 370 and in the Commission's Communication on the prevention of and fight against terrorist financing through enhanced national level coordination and greater transparency of the non-profit sector, COM(2005) 620.
62 OJ L 195, 27.7.2010, p. 5.
63 COM(2013) 843 final.

agreement will take place in 2021.

Today, a substantial part of **investigations** against all forms of crime and terrorism involve **encrypted information**. Encryption is essential to the digital world, securing digital systems and transactions. It is an important tool for the protection of cybersecurity and fundamental rights, including freedom of expression, privacy and data protection. At the same time, it can also be used as a secure channel for perpetrators where they can hide their actions from law enforcement and the judiciary. The Commission will work with Member States to identify possible legal, operational, and technical **solutions for lawful access** and promote an approach which both maintains the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime and terrorism.

As recognised by EU Ministers in their joint Statement of 13 November 2020[64], **availability of and access to digital evidence** is of the essence. A clear and robust framework for timely **cross-border access to electronic evidence** and investigative leads is required since digital evidence is needed in about 85% of all criminal investigations. The Commission calls on the co-legislators to ensure speedy and reliable access to e-evidence for authorities, by **urgently adopting the e-evidence proposals**. In addition, it is important that all Member States establish a connection to the **-Evidence Digital Exchange System (eEDES)** without undue delay. The Commission intends to lay down the future scope of eEDES in a legislative proposal on the digitalisation of judicial cooperation procedures[65].

The EU also needs strong rules for **cooperation with our international partners** in digital investigations. The Budapest Convention on Cybercrime is the international framework for such cooperation. The Commission will do its utmost for the finalisation of the negotiations in early 2021 on an updated framework (second additional protocol), which addresses the challenges of today's cyber-enabled crimes, including terrorism, through new and reinforced cooperation tools with the requisite safeguards for the protection of fundamental rights. The Commission will advance the negotiations on an EU-U.S. agreement on cross border access to electronic evidence as swiftly as possible, while ensuring that the outcome of the negotiations is compatible with the Union's internal rules on electronic evidence.

Furthermore, **battlefield evidence**, namely information uncovered and collected by military forces during battlefield operations or by private parties in a conflict zone, is paramount for **prosecution**. The Commission will continue to support Member States to use battlefield information to identify, detect and prosecute returning foreign terrorists fighters through the establishment of best practices[66], the exchange of information as well as possible project financing. In particular, the Commission and the European External Action Service will continue to support and strengthen the cooperation with key third countries such as the United States, including the exchange of information and ensuring the integration of battlefield information in the European security architecture and networks.

In order to ensure access to digital evidence and investigative leads, Member States rely on **data retention frameworks** to safeguard national and public security and in conducting

[64] https://www.consilium.europa.eu/en/press/press-releases/2020/11/13/joint-statement-by-the-eu-home-affairs-ministers-on-the-recent-terrorist-attacks-in-europe/

[65] Cf. Commission Work Programme 2021.

[66] Eurojust's 2020 Memorandum on Battlefield Evidence: https://www.eurojust.europa.eu/battlefield-evidence-increasingly-used-prosecute-foreign-terrorist-fighters-eu.

criminal investigations. The Court of Justice's recent rulings on data retention[67], while confirming that EU law precludes general and indiscriminate data retention, identified certain situations where **retention is permissible**, based on clear and proportionate obligations laid down in law and subject to strict substantive and procedural safeguards.[68] In their recent joint statement[69], EU Home Affairs Ministers underlined the importance of devising a way forward on data retention for crime fighting purposes. The Commission will assess available options to ensure that terrorists and other criminals can be identified and traced, while respecting EU law as interpreted by the Court of Justice.

Enhancing Member States' capabilities for investigation and evidence gathering is an important aspect of the criminal justice response to terrorism. The Commission will also assess the need for rules on the cross-border use of evidence in criminal proceedings. Moreover, there is a need to identify potential links between judicial proceedings (investigations and prosecutions) in terrorism cases in Member States. For this purpose, Eurojust has set up the **Counter-Terrorism Register** in 2019. The Register should become a proactive tool for ensuring coordination in cross-border judicial counter-terrorism proceedings and Eurojust be adequately resourced. To this end, in 2021, the Commission will adopt a **legislative proposal to improve information exchange and coordination in judicial proceedings in cross-border terrorism cases**, so as to make this exchange secure and efficient and enable Eurojust to react to it in a timely manner.

Strengthened support to victims of terrorism

Ensuring that victims of terrorism receive the necessary support, protection and recognition is a crucial part of responding to terrorism. The EU has adopted a robust set of rules on support and protection of **victims' rights,** including victims of terrorism[70]. In addition, the 2004 Compensation Directive[71] requires that Member States have in place national compensation schemes, including for victims of terrorism.

In January 2020, the Commission set up an **EU Centre of Expertise for victims of terrorism** as a two-year pilot project[72]. The Centre assists Member States and national victim support organisations with the application of EU rules, by providing guidelines, training activities and acting as a hub of expertise. The need for its continuation will be assessed by the end of 2021. A possible integration into a future EU Knowledge Hub on prevention of radicalisation will be explored as well. In June 2020, the Commission adopted its first **EU Strategy on victims' rights (2020-2025)**[73]. The Strategy pays special attention to the most vulnerable victims, including victims of terrorism. To improve cooperation and coordination for victims of terrorism, Member States should set up **national single contact points for**

---

67 Judgments in C-623/17, *Privacy International* and Joined Cases C-511/18, C-512/18 and C-520/18 *Quadrature du Net a.o*. of 6 October 2020.

68 Ibid. These include possibilities for the general retention of traffic and location data to safeguard against serious threats to national security that are genuine and present and foreseeable, the targeted retention of traffic and location data, based on persons and geographical criteria, for the purpose of combatting serious crime and prevention of serious threats to public safety, the general retention of IP addresses assigned to the source of a communication for a limited period of time and for the purposes of combating serious crimes, and the general retention of so-called civil identity data for the purposes of combatting crime in general.

69 Joint statement by the EU home affairs ministers on the recent terrorist attacks in Europe, https://www.consilium.europa.eu/en/press/press-releases/2020/11/13/joint-statement-by-the-eu-home-affairs-ministers-on-the-recent-terrorist-attacks-in-europe/

70 These include Victims' Rights Directive 2012/29/EU with rights for all victims of all crimes, and Directive (EU) 2017/541 on combating terrorism that responds more directly to the specific needs of victims of terrorism.

71 Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims.

72 https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/eu-centre-expertise-victims-terrorism_en.

73 COM(2020) 258 final.

victims of terrorism[74]. Under the Strategy, the Commission will assess the existing EU rules on victims' rights and, if necessary, propose legislative changes by 2022. The Commission will also assess how victims' access to compensation could be improved, including with regard to victims of terrorism in cross-border situations, who are residents of another Member State than that where the terrorist attack occurred. The Commission commemorates victims annually during the European Remembrance Day for victims of terrorism, to show unity and resilience against terrorism within our society.

KEY ACTIONS

The Commission will:

- Propose to revise the Prüm Decisions.
- Create a network of counter-terrorism financial investigators to improve cross-border financial investigations.
- Support Member States to use battlefield information to identify, detect and prosecute returning Foreign Terrorists Fighters.
- Propose a mandate to negotiate a cooperation agreement between the EU and Interpol.
- Support victims of terrorism, including through the EU Centre of Expertise for victims of terrorism.

The European Parliament and Council are urged to:

- Urgently adopt the e-evidence proposals to ensure speedy and reliable access to e-evidence for authorities.
- Examine the proposal to revise Europol's mandate.

5. REINFORCING INTERNATIONAL COOPERATION ACROSS ALL FOUR PILLARS

Counter-terrorism partnerships, including close cooperation with countries in the EU's neighbourhood, are essential to improve security inside the EU. The Council has called for further strengthening of the EU's external counter-terrorism engagement with a focus on the Western Balkans, North Africa and the Middle East, the Sahel region, the Horn of Africa, in other African countries where terrorist activities are increasing, and in key regions in Asia. Such engagement can help Member States in their work to close off terrorist activity, as well as working at a global level to combat terrorist organisations. In this regard, support from the CT/Security experts' network in EU Delegations in facilitating cooperation and promoting capacity building remains essential.

Cooperation with **Western Balkan partners** on counter-terrorism, including through relevant EU agencies, remains key. Fully implementing the Joint Action Plan on Counter-

[74] In line with the Council Conclusions on Victims of Terrorism, 4 June 2018 (9719/18).

terrorism for the Western Balkans[75], including integrating further the region into the activities of the Radicalisation Awareness Network is essential. The Commission will continue to prioritise cooperation in the area of police and judicial cooperation. Countering terrorism financing and protection of citizens and infrastructure is also key[76]. Cooperation with Western Balkan partners in the area of firearms will be stepped up in the coming years with their increased involvement in the Firearms priority of the European Multidisciplinary Platform Against Criminal Threats (EMPACT). The Commission will also continue to support financially the Western Balkan partners, Ukraine and Moldova with the implementation of the EU action plan on firearms trafficking.

Cooperation with priority countries in the **Southern Neighbourhood** should be further strengthened to reinforce measures to prevent and fight terrorism, including money laundering and terrorist financing, as well as the protection of public spaces and strengthening the rule of law. Southern Mediterranean countries are also a priority for the EU for developing police cooperation, considering their geographical proximity and the common security threats. The Commission has a mandate to negotiate international agreements with Algeria, Egypt, Israel, Jordan, Tunisia, Morocco, and Lebanon to exchange personal data with Europol in the framework of terrorism and serious organised crime. In addition, the Commission is currently seeking authorisation from the Council to open negotiations with ten[77] third countries on cooperation between Eurojust and those third countries in order to respond effectively to terrorism. Further afield, the Commission will increase cooperation in key countries in Sub-Saharan Africa and Asia on key areas across the strategy.

In particular, the EU should increase its engagement with relevant UN bodies such as the United Nations Office of Counter-Terrorism (UNOCT) as well as with other organisations like the OSCE or the Council of Europe on terrorism-related issues.

The Commission and the EEAS will also step up their engagement with **international organisations** such as NATO, Interpol, the Financial Action Task Force (FATF), as well as the Global Counterterrorism Forum, and with key strategic partners like the United States, Canada and New Zealand as well as the Global Coalition against Da'esh, to share experiences, foster closer cooperation, including with exchanges on the role of internet and social media, and enhance prevent-related research capacities. Globally, the EU will continue to empower civil society, grass-root and community actors in developing responses to address vulnerable individuals and support resilient societies.

The EU's approach to external security within the framework of the common Foreign and Security Policy (CFSP) and the Common Security and Defence Policy (CSDP) will remain an essential component of EU efforts to countering terrorism and violent extremism in order to strengthen stability and protect European security interests. The High Representative/Vice-President, supported by the EEAS will continue to play a key role in enhancing strategic and operational cooperation with third countries and international organisations, by making full use of its external tools, such as the High Level Counter-Terrorism Dialogues, the network of Counter-Terrorism/Security experts in EU Delegations and, where relevant, CSDP missions and operations.

---

[75] Joint Action Plan on Counter-Terrorism for the Western Balkans, 05.10.2018, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/news/docs/20181005_joint-action-plan-counter-terrorism-western-balkans.pdf

[76] Communication on a credible enlargement perspective for and enhanced EU engagement with the Western Balkans. COM (2018)65. p 10; https://www.consilium.europa.eu/en/press/press-releases/2020/10/23/joint-press-statement-eu-western-balkans-ministerial-forum-on-justice-and-home-affairs/ and also https://ec.europa.eu/home-affairs/sites/homeaffairs/files/news/docs/20181005_joint-action-plan-counter-terrorism-western-balkans.pdf

[77] Algeria, Armenia, Bosnia and Herzegovina, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey.

KEY ACTIONS:

The Commission and the High Representative/Vice-President, as appropriate, will:

- Step up cooperation with Western Balkan partners in the area of firearms
- Negotiate international agreements with Southern Neighbourhood countries to exchange personal data with Europol.
- Reinforce engagement with international organisations.
- Enhance strategic and operational cooperation with other regions such as the Sahel region, the Horn of Africa, with other African countries and key regions in Asia.

The European Parliament and Council are urged to:

- Authorise the opening of negotiations with Southern Neighbourhood countries to allow cooperation with Eurojust.

CONCLUSIONS

The threat from terrorism is real, dangerous, and, unfortunately, enduring. This calls for a renewed and sustained commitment to working together to counter the threat. It calls for unity in face of terrorism, which seeks to divide. This Counter-Terrorism Agenda for the EU sets out the way forward.

To pursue and coordinate this work, the Commission will appoint **a Counter-Terrorism Coordinator**, whose task will be to coordinate the various strands of EU policy and funding in the area of counter-terrorism within the Commission, including cooperation and coordination with Member States, in collaboration with the Council's EU Counter-Terrorism Coordinator, as well as the relevant EU Agencies, and the European Parliament.

The inclusive and rights-based foundations of our Union are our strongest protection against the threat of terrorism. An inclusive and welcoming society fully respectful of the rights of all is a society where terrorists will find it more difficult to radicalise and recruit. We must collectively uphold, reinforce and defend our democratic and fundamental values against those that seek to undermine them. For this, we need to invest in social cohesion, education and inclusive societies where everybody feels that his or her identity is respected and that they fully belong to the community as a whole.

This Counter-Terrorism Agenda for the EU builds on existing policies and instruments and will strengthen the EU's framework to further improve on anticipating threats and risks, preventing radicalisation and violent extremism, protecting people and infrastructures, including through external border security, and responding effectively after attacks.

Whilst this Agenda announces a series of new measures, implementation and enforcement remain key and there must be a common effort to ensure this, from swift adoption and application of the legal framework to speeding up the impact of measures on the ground. The Commission will work with Member States and keep the European Parliament, the Council and stakeholders informed and engaged in all relevant actions to implement the Counter-Terrorism Agenda for the EU.