Council of the European Union

Brussels, 27 February 2026
(OR. en)

6763/26

JAI 254
RELEX 293
COSI 36
CT 28
ENFOPOL 70
CRIMORG 49
CATS 9
COPEN 64
PROCIV 38
FRONT 52
HYBRID 27
IPCR 22
COTER 30
EUROPOL

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	27 February 2026
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2026) 101 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS ProtectEU: Agenda to prevent and counter terrorism

Delegations will find attached document COM(2026) 101 final.

Encl.: COM(2026) 101 final

EUROPEAN
COMMISSION

Brussels, 26.2.2026
COM(2026) 101 final

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

ProtectEU: Agenda to prevent and counter terrorism

1. Introduction

This Agenda, announced in the **ProtectEU: European Internal Security Strategy**[1], marks the start of a renewed effort to counter terrorism and violent extremism that knows no boundaries, be they physical or digital. Terrorism[2] and violent extremism[3] remain a persistent challenge for the EU and its Member States. The increasing links between terrorism and other crime areas, more fluid networks and less ideologically driven actors, as well as the blurred lines between online and physical operations, pose a particular challenge to defining and identifying terrorist offences. Against this complex threat landscape, **the best approach is united action,** and while Member States remain solely responsible for national security[4], the EU must work in unity with them.

While the EU has seen fewer large-scale coordinated terrorist attacks, **the threat has not gone away - it has evolved**. Between 2019 and 2023, the number of terrorist incidents more than doubled (from 57 to 120), before dropping to 58 in 2024[5]. Lone actors and small cells have been predominantly responsible for recent attacks. The overall **threat level remains high,** and it is shaped by **multiplying threat drivers**[6]. While **jihadist terrorism** remains the most prominent and lethal terrorist threat[7], terrorists and violent extremists are driven by a growing range of motivations, not always attached to a specific ideology, including the rejection of European democratic values, anti-semitism, or anti-Muslim hatred[8].

The EU has already taken action to tackle terrorism and violent extremism, using the **2020 Counter-terrorism Agenda for the EU[9]** as a roadmap towards creating a safer EU. In the decade since the spate of heinous attacks across Europe, including in Paris and Brussels, the EU has put in place a **comprehensive legal framework** to criminalise terrorist offences, address terrorist content online and restrict access to terrorist financing, firearms and explosives. We have strengthened our ability to **detect and stop terrorist travel** at external borders with modernised systems for security and border management, better information sharing and closer cooperation both within the EU and with non-EU countries.

---

[1] 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 ProtectEU: a European Internal Security Strategy, COM (2025) 148 final. The present Agenda complements deliverables under the European Preparedness Union Strategy JOIN (2025) 130 final, Preserving Peace – Defence Readiness Roadmap 2030 JOIN (2025) 27 final, European Democracy Shield: Empowering Strong and Resilient Democracies JOIN (2025) 791 final.

[2] Terrorist offences are defined in Article 3 of the Directive (EU) 2017/541 on combating terrorism as "terrorist offences are criminal acts which given their nature of context, may seriously damage a country or an international organization when they are committed intentionally and with a terrorist aim".

[3] There is no legal definition of violent extremism at EU level. Violent extremist acts do not meet the threshold set by the definition of terrorist offences; however, they pose a serious threat to security. A Project Based Collaboration on Violent Right-Wing Extremism (VRWE) developed a working definition.

[4] Article 4(2) of the Treaty on European Union.

[5] Europol, European Union Terrorism Situation and Trend Report (TE-SAT) 2025.

[6] Based on recent Europol TE-SAT and EU Intcen threat assessments (confidential).

[7] Europol, TE-SAT 2025.

[8] Other motivations include anti-LGBTQ+ hatred, misogyny, racism, anti-system ideologies, nihilism and "accelerationism", a range of ideologies that hold that the existing state of society is beyond redemption and requires destruction of the 'system' and a 'fresh start'.

[9] 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, COM (2020) 795 final.

EU agencies have provided operational support and tools to Member States, making **terrorism investigations and prosecutions more effective**, with over 2,000 arrests and over 1,800 convictions for terrorist offences[10] in the past five years. EU-level support structures, such as the **EU Knowledge Hub on Prevention of Radicalisation** and the **Protective Security Advisory Programme**, have allowed Member States to benefit from shared practices and expertise, **increasing resilience** across the EU. Building on these achievements, this Agenda, developed in close collaboration with Member States and other stakeholders, identifies the remaining gaps and sets out concrete steps to address them.

Geopolitical developments and external conflicts create increased risks and have an impact on the security of the EU. The 7 October 2023 Hamas attacks and the subsequent conflict in Gaza have fueled heightened hatred and incitement to violence across the ideological spectrum. Jihadist actors have instrumentalised these events through online misinformation and explicit calls to violence. Similar narratives have also been exploited by left-wing and right-wing extremist actors. This contributes to an increased risk of attacks. The Islamic State and its affiliates remain one of the main external threats to the EU due to their capacity to inspire attacks. The volatile situation in Syria raises security concerns due to the possible resurgence of the Islamic State organisation and the uncertain future of foreign terrorist fighters in detention facilities and camps in Northeast Syria. Terrorist organisations increasingly target humanitarian personnel and operations through violence, intimidation and obstruction.

In addition, in the context of **Russia's war of aggression** against Ukraine, Russia has undertaken a growing range of sabotage and hybrid actions against the EU. These actions violate Member States' territorial sovereignty, undermine the integrity of democratic institutions, and pose a direct threat to the safety and security of the civilian population. They have been coupled with coordinated influence activities by Russia-linked actors, including the spread of violent extremist and other divisive narratives in Europe. The conflict has also highlighted potential security risks linked to the return of foreign volunteers and Russian ex-combatants with combat experience.

The EU has also faced **complex threats sponsored by terrorist groups as well as by foreign state and non-state actors**. Hostile actors have been resorting to terrorist modi operandi such as placing improvised incendiary devices in air cargo, cyber-attacks and sabotage of critical infrastructure, as well as to the use of terrorists and violent extremists as proxies. Opportunistic links persist between terrorism, organised crime and cybercrime, using crime-as-a-service models, common recruitment pools, criminal marketplaces and underground banking networks[11]. The heightened connections between terrorism, cyber-crime, hostile foreign interference and organised crime pose challenges in attribution of criminal responsibility and coordinating national and EU level responses.

The **number of minors involved in terrorism and violent extremism** has increased sharply across Europe. In 2024, almost one third of terrorist suspects in the EU were under 20, with the youngest only 12 years old. Most of these minors have been linked to jihadist terrorism, although violent right-wing extremism has gained traction, particularly through accelerationist

[10] Europol, TE-SAT reports 2021-2025.
[11] Europol, EU Serious and Organised Crime Threat Assessment (EU-SOCTA), 2025; Beneath the Surface: Terrorist and Violent Extremist Use of the Dark Web and Cybercrime-As-A-Service for Cyber-Attacks | Office of Counter-Terrorism.

networks, "active clubs"[12] and online extremist networks[13] disseminating violent content and coercing vulnerable minors into acts of self-harm and violence. Mixed ideologies have been prominent, with a fascination for violence as a primary motive for many lone actor attacks.

Terrorists and violent extremists increasingly **exploit the online ecosystem and new technologies, social media and gaming platforms** to share harmful content, spread disinformation, radicalise, raise funds, and recruit. Algorithmic amplification of extremist content furthers radicalisation. Terrorist actors coordinate plans on end-to-end encrypted (E2EE) communication platforms and finance their networks and attacks with **cryptocurrencies**, non-fungible digital assets (NFTs) and "digital hawala"[14]. Generative AI is abused to create instruction manuals for attacks. 3D-printing technology (e.g. to manufacture firearms) and the increased use of unmanned aircraft systems (UASs /drones) further exacerbate the threat.

Building on extensive stakeholder consultations and the recent Council Conclusions[15] on terrorism, the Agenda combines important ongoing activities with new initiatives to keep up with the fast-evolving threat landscape. It sets out specific actions to **anticipate threats, prevent radicalisation, protect people both online and offline, ensure swift, coordinated responses to attacks,** and **strengthen the global fight against terrorism** in line with international law, including human rights law and humanitarian law.

The most effective response to terrorism is one that demonstrates the commitment to our values under attack; hence all actions are rooted in **respect for fundamental rights**. To complement and complete that response, Member States are invited to adopt and regularly update their national strategies, following the strategic framework set by this Agenda.

2. Pillars to counter terrorism and violent extremism

2.1 Anticipating threats

Security starts with **effective anticipation and foresight**. The EU has built strong counter-terrorism situational-awareness capacities. The **EU Single Intelligence Analysis Capacity (SIAC)**, the single point of entry for Member State intelligence contributions, delivers timely threat assessments, while **Europol** produces regular trend reports based on law enforcement information.

The High Representative for Foreign Affairs and Security Policy ('High Representative') will prioritise the **strengthening of SIAC** in terms of resources and capacities. In addition to the **roll-out of secure communication channels** and the finalisation of negotiations on the **proposed Regulation on information security** in institutions, bodies, offices and agencies of the Union, the Commission and the High Representative will work on **further strengthening**

[12] Active clubs are loosely organised extremist networks centred on fitness or martial arts, serving as hubs for ideology, cohesion, and recruitment in violent right-wing circles.
[13] Known as "764" or "Com" networks.
[14] Digital hawala provides a method of cross-border, pseudo-anonymous transfers through various digital methods (blockchain technology, mobile money etc.), resembling hawala's physical informal network, while introducing added layers of security. (TE-SAT 2025).
[15] Council Conclusions of 9 June 2022 on protecting Europeans from terrorism: achievements and next steps Council Conclusions of 12 December 2024 on future priorities for strengthening the joint counterterrorism efforts of the European Union and its Member States.

EU staff awareness to foster a **'need to share' culture** whilst preserving the 'need to know' principle for classified information.

The dynamic and unpredictable nature of emerging threats requires strengthened law enforcement anticipation capacities. As set out in the ProtectEU Internal Security Strategy, the Commission will propose to enhance **Europol's analytical support, including open-source intelligence (OSINT) capacities**. Where possible, Europol's trend reports, situational briefs, and thematic analyses could be provided in non-classified formats to raise public awareness on emerging trends in support of early detection and prevention efforts. In addition, the threat analyses the Commission is preparing as announced in ProtectEU Internal Security Strategy will also help identify the emerging threats and policy responses to counter terrorism and violent extremism.

Foresight is equally essential to identify the risks and opportunities stemming from new technologies[16]. The **Joint Research Centre**'s work will continue to guide security research. To embrace the potential of new technologies for law enforcement and prepare to counter their misuse by terrorists and violent extremists, the Commission will **reinforce security research under Horizon Europe and Internal Security funding** with dedicated calls in 2026 and beyond. Research priorities will include early detection capacities and innovation in technologies, such as AI, tackling extremist use of online platforms, new terrorist financing methods (e.g. crypto-assets), and protecting citizens and public spaces from threats posed by the use of explosives, drones and 3D-printed weapons, as well as vehicle ramming and use of bladed weapons. To ensure the uptake of research results, the Commission will also **support the testing and deployment of EU-funded solutions to equip law enforcement with state-of-the-art tools and methodologies** for effective prevention, detection and response to terrorism and violent extremism.

KEY ACTIONS

The Commission will:

- Support the roll-out of secure communication channels between EU institutions, bodies and agencies
- Reinforce security research under Horizon Europe and Internal Security funding
- Support testing and deployment of EU-funded solutions to equip law enforcement with state-of-the-art tools

The High Representative will:

- Strengthen SIAC as a matter of priority in line with the Joint Paper of the High Representative and the Member States

Europol will:

- Enhance analytical support and open-source intelligence (OSINT) capacities

The European Parliament and the Council are encouraged to:

- Finalise negotiations on the Regulation on information security in institutions, bodies, offices and agencies of the Union

2.2 Preventing radicalisation

Preventing radicalisation means tackling its drivers before they take root. It requires **a whole-of-society approach**, engaging stakeholders across education, social, cultural and youth

[16] See European Commission Joint Research Centre Publication – Emerging risks and opportunities for EU internal security stemming from new technologies (2025) EUR 40239 JRC139674.

services, law enforcement, prisons and probation services, local communities, civil society organisations and online environments. Establishing the **EU Knowledge Hub on Prevention of Radicalisation** ('Knowledge Hub')[17] in June 2024 and allocating EUR 60 million over four years marked a step change in EU prevention policy.

The Knowledge Hub connects over 6,000 policymakers, researchers and practitioners across Europe and develops **guidance for policy makers and practitioners, practical tools, training and tailor-made support services.** It operates under the Strategic Orientations[18] set by Member States that will be updated in 2027. This Agenda sets out concrete tasks for the Knowledge Hub and ensures that it delivers fully on its mandate by translating these into operational support for Member States, helping them anticipate emerging risks and identify country-specific responses to radicalisation.

2.2.1. Developing a prevention toolbox for minors

The consequences of minors' involvement in radicalisation and terrorism are far-reaching, affecting not only the minors involved, but also communities and societies as a whole. To address the concerning rate of minors being radicalised across Europe, the Commission will build on the activities of the Knowledge Hub and provide strategic guidance on **preventing radicalisation of minors**. It will focus on early detection, strengthening protective factors, resilience through education[19] and social integration, in particular of vulnerable minors, support for families and communities, safe online engagement, and cooperation across sectors, also building on the work of the existing networks of the Safer Internet Centres in Member States and candidate countries.

The Commission recognises that **mental health challenges** can make minors more vulnerable to extremist narratives, violence and recruitment. It will therefore promote closer cooperation between prevention actors and mental health services in an integrated approach to child protection[20]. In this vein, Member States are encouraged to integrate psychosocial expertise and support into their prevention frameworks.

2.2.2. Building resilient societies

To strengthen the resilience of communities, the Commission is launching the **Community Engagement and Empowerment Programme (CEEP)** allocating EUR 5 million to equip civil society and practitioners with digital skills for effective online interventions and to amplify the voices of youth engaged in prevention.

Protecting all faith communities from hatred, discrimination and violence remains a core European commitment. The Commission will accelerate the implementation of the **EU Strategy on Combating Antisemitism and fostering Jewish Life[21]** and build a network to counter antisemitic hate speech online. In line with this Strategy, the SIAC will continue to include analyses of specific threats to Jewish people, communities and places of worship in their regular threat assessments. Member States are encouraged to follow the

[17] The Knowledge Hub on Prevention of Radicalisation.
[18] Strategic Orientations on a coordinated EU approach to prevention of radicalisation.
[19] For further measures on fostering resilience through education, including those on media, digital literacy and citizenship see: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Democracy Shield: Empowering Strong and Resilient Democracies, JOIN (2025) 791 final. European Democracy Shield, JOIN (2025) 791 final.
[20] In line with the Commission Recommendation (EU) 2024/1238 of 23 April 2024 on developing and strengthening integrated child protection systems in the best interests of the child.
[21] EU Strategy on combating antisemitism and fostering Jewish life (2021 – 2030), COM/2021/615 final.

recommendations from the Project-Based Collaboration on Antisemitism in Preventing and Countering Violent Extremism[22].

To strengthen the criminal law response at EU level to all forms of hatred, including rising anti-Muslim hatred, the Commission is considering a legislative initiative to harmonise the **definition of hate offences committed online**[23].The Commission will cooperate with Europol to improve **AI-assisted detection of extremist content**, shared threat indicators, and faster cooperation between platforms, law enforcement and researchers to identify AI-generated propaganda and coordinated radicalisation campaigns.

2.2.3. Addressing radicalisation in prisons, prison leavers and managing the return of Foreign Terrorist Fighters and their family members

In view of the possible release of prisoners who have served their sentence but may be **radicalised**,[24] it is necessary for there to be stronger coordination and tailored reintegration measures. Member States should **strengthen information sharing** between prison, probation and law enforcement authorities and implement evidence-based disengagement and reintegration programmes.

The Knowledge Hub will support these efforts by **developing tools to assess and manage risks in the pre-release phase**, while the Commission will provide **guidance** to support national approaches to radicalised prison leavers.

To manage the complex challenges linked to **returning foreign terrorist fighters and their families,** Member States are encouraged to continue to prevent departures to conflict areas and pursue effective prosecution of returning foreign terrorist fighters. The Knowledge Hub will support Member States with tools to assess risks and manage returnees safely, and training on rehabilitation and reintegration, with a focus on protecting children in their best interest.

2.2.4. Supporting victims of terrorism

Victims of terrorism face long-lasting consequences and need specialised support. The co-legislators have recently reached agreement on the proposed **revision of the Victims' Rights Directive**[25] that will strengthen the protection of the rights of victims of terrorism, complemented with a **new EU Strategy on Victims' Rights**. The Commission will also enhance the visibility of the **EU Remembrance Day for victims of terrorism and will support victims' associations** by promoting their active role in prevention programmes.

KEY ACTIONS

The Commission, in cooperation with the EU Knowledge Hub, will:

[22] European Commission Set of Recommendations from the PBC Antisemitism in Preventing and Countering Violent Extremism (P/CVE) March 2025. Following up to these Recommendations, the EU Knowledge Hub has produced a Handbook on key symbols, narratives and reporting mechanisms that will be published.

[23] At EU level, the current legal framework provided by the Council Framework Decision on combating certain forms and expressions of racism and xenophobia (Council Framework Decision 2008/913/JHA) and by the Directive on combating violence against women and domestic violence (Directive (EU) 2024/138) only covers hate offences based on racist and xenophobic grounds and cyber incitement to violence or hatred based on gender, respectively.

[24] According to Europol's assessments (non-public data).

[25] Proposal for a Directive of the European Parliament and of the Council amending Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA COM/2023/424 final.

- Develop a Prevention Toolbox for Minors, including a Parents' Guide to Protecting Young Minds from Radicalisation in the online environment and practical models for hotlines and call centres for reporting and acting on signs of radicalisation
- Develop standardised procedures and a common risk evaluation methodology for radicalised inmates in the pre-release phase

The Commission will:

- Launch the Community Engagement and Empowerment Programme together with this Agenda
- Develop recommendations on prevention of radicalisation of minors and on prison leavers
- Present a new EU Strategy on Victims' Rights
- Cooperate with Europol to improve AI-assisted detection of extremist and radicalisation campaign content

Member States are encouraged to:

- Embed prevention of radicalisation in education and sport, drawing on the recommendations, tools and good practices developed at EU level
- Strengthen strategic communication and awareness campaigns, drawing on support provided by the EU Knowledge Hub
- Strengthen information sharing and implement disengagement and reintegration programmes for prison leavers
- Prevent departures to conflict areas and prosecute returning foreign terrorist fighters

2.3 Protecting people online

Over the past years, the EU has built one of the most advanced regulatory frameworks in the world to counter terrorist activity online, complemented by the voluntary cooperation of Member States, online platforms and Europol.

Yet the threat continues to evolve. Extremist networks adapt quickly, exploit emerging technologies and shift from open platforms to exploiting closed chats and encrypted services. This can create serious challenges for detecting and preventing terrorist plans, for mapping terrorist networks and their supporters, and for investigating and prosecuting terrorist activities. In addition, terrorist materials proliferate more easily, requiring smarter detection tools to ensure that identified terrorist content does not resurface elsewhere. The Commission will strengthen enforcement of the Digital Services Act (DSA) and support effective implementation of the Terrorist Content Online (TCO) Regulation, close remaining gaps, and ensure faster, more coordinated responses to keep the online space safe and resilient against misuse, while ensuring respect for fundamental rights. As announced in the ProtectEU Internal Security Strategy, the Commission will also put forward an **Action Plan on the Protection of Children against Crime**, which will include measures to address radicalisation and recruitment into crime both online and offline.

2.3.1. Making full use of regulatory frameworks to tackle terrorist and extremist content online

The **Terrorist Content Online (TCO) Regulation** has been instrumental in countering the dissemination of terrorist material, enabling rapid removal of terrorist content. Its importance

was demonstrated following the 7 October 2023 Hamas attacks on Israel, when several hundred removal orders were issued in relation to terrorist content[26].

By December 2025, Member States' authorities had already sent 2,032 removal orders and more than 97,900 referrals for voluntary removal[27]. To further support implementation, Europol will develop a European **hash-sharing database** (database of digital footprints ('hashes')) for terrorist and violent extremist content. This will enable Member States and hosting service providers to securely flag, match and remove content across platforms, including content removed under the TCO Regulation.

The Commission will conclude the evaluation of the TCO Regulation by the end of 2026. Based on the evaluation, the Commission will explore a further strengthening of the TCO Regulation to keep it fit for purpose and will simplify it where possible, while preserving safeguards to effectively protect fundamental rights. In parallel, the Commission will ensure the rigorous enforcement of other relevant legislation that safeguards the digital space, such as the **Digital Services Act (DSA)** and the **Audiovisual Media Services Directive.**

The TCO Regulation and the DSA form a reinforced and mutually supportive architecture[28] to counter terrorist activity and violent extremism online. While the DSA establishes a horizontal framework of due diligence obligations for online intermediaries to address illegal content online and its algorithmic amplification, and mitigate systemic risks associated with their services, the TCO Regulation sets sector-specific requirements for terrorist content and rapid operational tools for removal. Very large online platforms and search engines have already recognised terrorism and violent extremism online as systemic risks[29]. The Commission will closely monitor the implemented mitigation measures and enforce the DSAwhere necessary.

In addition, the European Board for Digital Services plays a key role in ensuring the effective and consistent enforcement of the DSAacross the Member States, including the service providers' obligations to address illegal radicalising and violent extremist content. The **AI Act**[30] harmonises the rules for AI, including for high-risk AI tools. The Commission will adopt guidelines to support law enforcement and the judiciary in improving their ability to detect and prevent threats with certified trustworthy AI systems for high-risk uses, while respecting fundamental rights. The **Apply AI Strategy** will further support the development and uptake of AI solutions for internal security purposes. As from August 2026, the AI Act's prohibitions will be applied, banning from the EU market AI systems and chatbots that manipulate users, including where such manipulation leads to radicalisation into committing terrorist offences or other significant harms. Furthermore, if large generative AI models amplify harmful manipulation leading to user radicalisation, providers will need to assess and mitigate such risks, and the European AI Office will engage with them to address such issues.

2.3.2. Working with industry

Voluntary cooperation with online service providers is indispensable in reacting to emerging trends and an evolving online threat landscape. For this, the **EU Internet Forum** is the

[26] Europol, Point d'Entrée pour le Retrait de Contenus terroristes sur Internet (PERCI) database figures.
[27] Ibid.
[28] Commission evaluates the Digital Services Act's interaction with other EU laws and its designation threshold for VLOPs and VLOSEs | Shaping Europe's digital future
[29] Digital Services Act report lays out landscape of systemic risks online | Shaping Europe's digital future.
[30] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

Commission's main avenue, and it will be strengthened further. This Forum is a prime example of private-public collaboration bringing together EU Member States' ministries, law enforcement authorities, civil society and online service providers, including social media platforms. This allows for an exchange on priorities and supports coordinated and comprehensive responses when it comes to countering radicalisation and limiting the spread of terrorist and violent extremist content.

The Commission will also work with the **European Board for Digital Services**, in cooperation with relevant law enforcement stakeholders and companies, to reinforce efforts against the dissemination of terrorist and violent extremist content, as well as online radicalisation, under the DSA. This may include, where necessary, specific actions supporting online service providers in complying with and enforcement of the DSA. Such actions may include identifying effective mitigation measures to address systemic risks, the development and implementation of voluntary guidelines and code of conducts or voluntary cooperation frameworks. They may also involve issuing recommendations or advice to the Digital Services Coordinators to support coordinated action at national level, in particular with regard to services that do not qualify as very large online platforms or search engines. They may also focus on enhancing and streamlining the exchange of relevant information on trends and emerging risks associated with the services provided by online intermediaries.

Conspiracy theories, extremist narratives and extreme violent and borderline content fuel radicalisation and polarisation. In the framework of the EU Internet Forum, Europol will facilitate cooperation with online service providers to improve handling of such content, when incorporated in narratives that incite to or recruit for terrorism[31], while upholding fundamental rights.

Terrorists and extremist actors increasingly exploit **online gaming** to spread propaganda, desensitise to violence, and recruit followers, including minors. To counter this, the EU Internet Forum will foster **cooperation between the gaming sector and law enforcement** focused on safeguarding minors and explore developing **guidance to prevent recruitment** in these spaces. Europol will develop **a dedicated capability** to monitor and analyse such misuse. In addition, the Commission will address the security aspects of online gaming as part of its overall strategy on video games, to be issued in 2026.

In parallel, the Commission will monitor that online service providers' deliver on their commitments under the **Code of conduct on countering illegal hate speech online+**.

2.3.3. Ensuring effective and coordinated crisis response online

The **EU Crisis Protocol** provides a voluntary framework for cooperation between law enforcement authorities and online service providers following a terrorist attack with major impacts online. It will be revised into an **EU Online Crisis Response Framework** and enable Member States to use it where an incident leads to heightened online activity related to an attack, and to anchor it in the DSA thereby ensuring a coordinated response that leverages the DSA's crisis provisions. Europol will facilitate operational crisis response with a technical platform enabling swift coordination. The Commission will also develop **guidance** for law enforcement and online service providers **on handling bystander footage** of terrorist attacks, safeguarding the dignity of victims.

[31] Deconfliction refers to the process of cross-checking operational information and coordinating investigative activities among competent authorities to avoid overlap or interference between parallel investigations.

The European Board of Digital Services is working on practical advice to support Digital Services Coordinators in monitoring compliance with relevant obligations. These obligations require hosting service providers to promptly alert law enforcement or judicial authorities. This applies when providers become aware of information giving rise to a suspicion that a criminal offence involving **a threat to life or safety of a person** is taking place, has taken place or is likely to take place. Such offences may also include forms of terrorism and illegal violent extremism.

KEY ACTIONS

The Commission will:

- Explore the revision of the TCO Regulation, based on its evaluation
- Continue to monitor and step up the enforcement of the obligations of very large online platforms and search engines under the DSA to mitigate systemic risks related to the dissemination of terrorist and violent extremist content
- Facilitate closer cooperation between the European Board for Digital Services and law enforcement authorities and companies on combatting terrorism and violent extremism online
- Develop a new workstream in the EU Internet Forum to strengthen online service providers' user support mechanisms and positive interventions to prevent radicalisation online
- Integrate the EU Online Crisis Response Framework under the DSA
- Develop guidance on handling bystander footage of terrorist attacks

Europol will:

- Develop a European hash-sharing database for terrorist and extremist content
- Facilitate EU-level cooperation with online service providers to improve the handling of forms of illegal content connected to terrorism and other harmful content
- Monitor extremist misuse of gaming platforms and provide regular assessments
- Establish a crisis response platform

Member States are encouraged to:

- Ensure effective implementation and enforcement of the TCO Regulation and the DSA

Online service providers are urged to:

- Regularly review and update their terms and conditions to reflect evolving threats
- Strengthen their monitoring mechanisms to detect and swiftly remove terrorist content
- Step up cooperation with national authorities and Europol to ensure timely exchanges and coordinated responses

2.4 Protecting people in the physical environment

Recent years have seen significant progress across the EU to protect people, public spaces and critical infrastructure from terrorist attacks. The EU provides practical support through its **EU Protective Security Advisors**, who can advise on vulnerabilities and provide specific recommendations for improvement. In parallel, the **EU counter-drone programme**[32] has been building up law enforcement capabilities to tackle the threat posed by non-cooperative drones.

[32] Launched with the Communication from the Commission to the Council and the European Parliament on countering potential threats posed by drones COM/2023/659 final.

The adoption of the **Directive on the resilience of critical entities**[33] in 2022 was a key step, shifting the EU from a 'protection' to a 'resilience' approach.

However, terrorists have continued to expand their means to commit attacks: from new technologies, such as drones and 3-D printed weapons, to unsophisticated low-cost methods, such as bladed weapons and vehicle ramming. Access to the means to carry out attacks needs to be further restricted and the tools to protect public spaces and critical infrastructure expanded. In parallel, to address terrorist travel and the potential return of foreign terrorist fighters, we need to upgrade the existing EU measures to secure external borders and impede terrorist travel.

2.4.1. Impeding terrorist travel

Strong protection of external borders is the EU's first line of defence against terrorist travel. Once fully operational, the **new EU large-scale information systems**, notably the Entry/Exit System (EES), the European Travel Authorisation System (ETIAS), the revised Visa Information System (VIS) and the interoperability framework will provide Member States with essential information on individuals from third countries entering the EU. These systems will also support national authorities in stopping individuals posing security risks, including terrorist suspects.

Identifying foreign terrorist fighters and terrorist suspects at borders also requires timely access to data. To this end, the Commission, together with Europol, will **strengthen cooperation with trusted third countries to obtain biographic and biometric data on individuals that might pose a terrorist threat,** for insertion into the Schengen Information System (SIS) in full compliance with applicable EU and national legal frameworks. To strengthen this information flow, the **SIS 'information alert'[34] is planned to enter into operation in 2026.** Upon Europol's proposal and based on information from third countries, Member States will be able to enter relevant alerts in SIS, ensuring that information on terrorists and suspects is accessible to border and law enforcement authorities[35].

Following the recent Council Conclusions on future priorities for strengthening the joint counter-terrorism efforts[36], in the context of the overall evaluation of the Schengen Information System, the Commission will **propose a way forward on a 'post-hit procedure'** to further share hits on terrorism-related alerts with volunteering Member States. It will also assess **the application of refusal of entry alerts**[37] and update the SIS Handbook as necessary. Moreover, the Commission will work closely with Member States to advance cooperation and information sharing on individuals potentially posing a terrorist or violent extremist threat ('**Gefährder**')[38].

---

[33] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC *OJ L 333, 27.12.2022*.

[34] Regulation (EU) 2022/1190 of the European Parliament and of the Council of 6 July 2022 amending Regulation (EU) 2018/1862 as regards the entry of information alerts into the Schengen Information System (SIS) on third-country nationals in the interest of the Union *OJ L 185, 12.7.2022*.

[35] Ibid.

[36] Council Conclusions of 12 December 2024 on future priorities for strengthening the joint counterterrorism efforts of the European Union and its Member States.

[37] Article 24 of Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters *OJ L 312, 7.12.2018*.

[38] Council Note A shared understanding of when a person should be regarded as a potential terrorist or violent extremist threat ("Gefährder") ST 8807 2024 REV 1 – NOTE.

As announced in the ProtectEU Internal Security Strategy, the Commission will assess measures to **enhance information exchange for law enforcement and border management purposes with trusted third countries.** For security and border management purposes, this could be implemented via a technical solution to allow controlled and limited exchange of a selected sub-set of data from EU databases, on the basis of an international agreement and in a reciprocal manner. For law enforcement purposes, this could be implemented by extending the EU's automated police information exchange framework (Prüm) and the Schengen Information System (SIS) to trusted third countries, enhancing cross-border investigations while fully upholding fundamental rights, EU data protection and security standards.

The new **screening process**[39], entering into application in June 2026, will facilitate the identification of third-country nationals who have crossed the external borders illegally or are staying illegally on Member States' territory without having undergone entry checks. Systematic checks will have to be conducted to assess whether they pose a security risk. For individuals posing a terrorist threat, criminal law and extradition procedures may be launched. The Commission will promote **the efficient return of individuals posing a security risk,** by facilitating the swift adoption of firmer rules in the **Return Regulation proposal**[40] and through the work of the Return Coordinator and the High-Level Network for Returns. The Commission also encourages Member States to continue enhancing the **cooperation and coordination between counter-terrorism and migration and asylum authorities**.

In addition**, advance travel information** (such as Advanced Passenger Information (API) and Passenger Name Record (PNR) data) is indispensable for law enforcement authorities to effectively plan and efficiently deploy counter terrorism efforts both at the external borders and within the EU territory. The current EU framework is limited to commercial air transport, resulting in legal and operational loopholes that terrorists may exploit to move across the EU. The Commission, in close coordination with Member States and the transport industry, is exploring **options to expand the current framework** to other modes of transport such as maritime and land transport, and to private flights, and to strengthen the PNR Directive, subject to its evaluation[41].

2.4.2. Restricting access to means used to commit attacks

Further restricting access to means used to commit attacks is essential. Recent seizures, including of 3-D printed firearms, demonstrate the persistent availability of weapons notably among right-wing terrorists and violent extremists[42]. The Commission will present a **legislative proposal to harmonise the criminalisation of firearms trafficking and other firearms-related offences** in early 2026, including the illicit creation, possession and dissemination of blueprints to manufacture 3-D printed firearms.

Terrorists and violent extremists also continue to show interest in homemade explosives, evidenced in manuals and instruction material circulating online. To address these challenges,

[39] Regulation (EU) 2024/1356 of the European Parliament and of the Council of 14 May 2024 introducing the screening of third-country nationals at the external borders *OJ L, 2024/1356, 22.5.2024*.
[40] Proposal for a Regulation of the European Parliament and of the Council establishing a common system for the return of third-country nationals staying illegally in the Union, and repealing Directive 2008/115/EC of the European Parliament and the Council, Council Directive 2001/40/EC and Council Decision 2004/191/EC COM/2025/101 final.
[41] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime *OJ L 119, 4.5.2016*.
[42] Europol, TE-SAT 2025.

the Commission is **reviewing the EU Regulation on explosives precursors**[43]. The recently concluded **evaluation of the Pyrotechnics Directive**[44] identified shortcomings in public security, notably the broad accessibility of high-risk professional fireworks to unauthorised users. The Commission is assessing options, including a potential **review** of the Directive.

Chemical, biological, radiological and nuclear (CBRN) risks in the context of terrorism are low-likelihood, but high-impact events for which EU-wide preparedness is key. The Commission will present a **new CBRN Preparedness and Response Action Plan** in 2026. It will, among others, propose a more robust EU-level programme for training and exercises, and explore possibilities to address misuse of novel technologies such as nucleic acid synthesis and AI-enabled biotechnology. In parallel, the **EU Stockpiling Strategy** and the **EU Medical Countermeasures Strategy** will foster health preparedness to mitigate the impact of CBRN risks.

2.4.3. Addressing the threat posed by drones

The EU also needs to be prepared to tackle threats resulting from the use of new and emerging technologies, such as the malicious use of drones by terrorist actors. Drones, whether airborne, maritime surface, underwater or terrestrial, pose significant challenges for the protection of critical infrastructure and public spaces. Building on the 2023 Communication on countering potential threats posed by drones[45] as well as the Drone Strategy 2.0[46], the Commission recently put forward a comprehensive cross-sectoral **EU Action Plan on drone and counter drone security.** The new Action Plan will further enhance capabilities of law enforcement, border and coast guards to counter threats posed by drones with specialised counter-drone training, possible development of a drone incident platform, as well as pooling and sharing of resources.

2.4.4. Protecting public spaces

Public spaces remain main targets of terrorist attacks. It is therefore essential to adopt a security-by-design principle in planning of urban areas, public spaces and places of worship across Europe.[47] Security by design should be a shared responsibility built on strong public-private cooperation. Therefore, the Commission will assess and examine options to introduce a **"commitment to protect" by operators of public spaces** (e.g. sports venues, music halls, places of worship) to implement risk-based security measures against potential terrorist threats at public venues.

In parallel, the Commission is investing **EUR 30 million in projects aimed at improving the overall security of public spaces** with a focus on places of worship of all faiths, CBRN threats, firearms trafficking, explosives detection dogs and non-cooperative drones. EUR 5 million of that are earmarked for the protection of Jewish places of worship, with projects scheduled to

[43] Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors, amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013 *OJ L 186, 11.7.2019*.
[44] Commission Staff Working Document Evaluation of Directive 2013/29/EU of the European Parliament and of the Council of 12 June 2013 on the harmonisation of the laws of the Member States relating to the making available on the market of pyrotechnic articles (recast) SWD (2025) 269 final.
[45] Communication from the Commission to the Council and the European Parliament on countering potential threats posed by drones COM/2023/659 final.
[46] Communication from the Commission to the Council and the European Parliament A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe COM (2022) 652 final.
[47] European Commission Security by Design: Protection of public spaces from terrorist attacks (2023) JRC131172.

deliver results by 2027.[48] The Commission will continue to support the protection of places of worship as part of the proposed tripling of funding for Home Affairs policies under the next MFF.[49]

To further strengthen public-private cooperation, the Commission will upgrade the **EU Forum on the protection of public spaces**[50] to create a consultative body to support policymaking. Together with the Forum, the Commission will update the **EU Guidelines on public-private partnerships to protect public spaces** and **national best practices of public space protection measures**, with a particular focus on protecting places of worship, building on the results of EU-funded projects in this area.

The **Protective Security Advisory programme** has been instrumental in building capabilities to conduct vulnerability assessments of public spaces and critical infrastructures, with **more than 50 advisory missions** performed since 2022. To meet the growing demand by Member States, the Commission will assess the programme in 2026 and aims to strengthen it both financially and operationally under the new Multiannual Financial Framework.

Following the Commission Recommendations for x-ray and metal detection[51], the Commission, together with Member States, will develop further **voluntary performance requirements for detection equipment outside aviation** and launch **voluntary verification and certification schemes** for chemicals, explosives and firearms detection, as well as detection dogs.

2.4.5. Resilience of critical entities, transport and supply chain security

While Member States reported only four attacks classified as "terrorist" against critical infrastructure in 2024[52], there are growing concerns about incidents linked to hybrid campaigns and potential acts of sabotage by hostile state actors and their proxies. To increase resilience, all Member States should urgently transpose and implement the Critical Entities Resilience (CER) Directive and the NIS2 Directive.[53] In cooperation with Member States, **EU-level exercises** will be organised to test the physical and cyber resilience of critical infrastructure in significant cross-border incidents. To support the effective implementation of the CER Directive and strengthen the cross-border and cross-sectoral resilience of critical infrastructure against man-made threats, the Commission will make **EUR 15 million available for projects** and adopt **guidelines** to support critical entities identified by Member States in their resilience-enhancing measures. In addition, the Commission proposed to further enhance the protection and resilience of critical entities in the Connecting Europe Facility and the European Competitiveness Fund under the next MFF.

---

[48] See projects funded under the ISF call for proposals on the protection of public spaces: ISF-2024-TF2-AG-PROTECT.

[49] Proposal for a Regulation of the European Parliament and of the Council establishing the Union support for internal security for the period from 2028 to 2034

[50] The EU Forum on the protection of public spaces brings together regional and local authorities, private operators of public spaces, private sector and faith-based organisations to exchange best practices on protection measures.

[51] Commission Recommendation (EU) 2022/1341 of 23 June 2022 on voluntary performance requirements for X-ray equipment used in public spaces (outside aviation) C/2022/4179.
Commission Recommendation (EU) 2023/1468 of 10 May 2023 on voluntary EU performance requirements for metal detection equipment used in public spaces (outside aviation) C/2023/3039.

[52] Europol, TE-SAT 2025.

[53] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) *OJ L 333, 27.12.2022*.

Transport remains a high-profile target, and it is expected that the threat will continue to evolve with diverse modi operandi to stage attacks. Based on the comprehensive mapping of aviation security risks, the Commission will develop a **new EU future-proof aviation security baseline,** inter alia by strengthening the aviation security legislation (AVSEC)[54] to enable immediate response while maintaining the one-stop security area within the EU. The Commission has also proposed to establish an **EU aviation security occurrence reporting system** to facilitate information sharing on security occurrences and incidents, building on existing mechanisms, and to develop an EU multi-agency threat alert mechanism to respond to potential emerging crises in transport and supply chains.

As a result of air cargo incidents, the EU civil aviation security rules have been modified[55] to **enhance resilience** and **protection of the air cargo and mail supply chain.** To mitigate attacks and sabotage targeting railways, the Commission and the EU Agency for Railways (ERA) will strengthen the robustness of the rail traffic management system to ensure continued operations in case of system-wide failures.

Under the **EU Ports Strategy**, the Commission will further strengthen maritime security legislation to effectively address emerging threats, enhance EU supply chain security, and assess introducing background checks for port workers. The Commission will also work with law enforcement and customs authorities, international organisations, third countries, and private sector to mitigate CBRN threats in maritime supply chains.

KEY ACTIONS

The Commission will:

- Propose a way forward on a 'post-hit procedure' in the SIS evaluation
- Support the entry into operation of information alerts in the SIS
- Explore options to strengthen and expand the EU travel information (API/PNR) framework
- Present a legislative proposal to harmonise the criminalisation of firearms related offences
- Review the Regulation on explosives precursors
- Present a new CBRN Preparedness and Response Action Plan
- Implement the EU Action Plan on drone and counter drone security
- Assess and examine options to introduce a "commitment to protect" for operators of public spaces
- Upgrade the Protective Security Advisory Programme under the new MFF

The Commission, together with Europol, will:

- Strengthen its cooperation with trusted third countries to obtain data of sufficient quality (biographic, biometric and contextual) on individuals that might pose a terrorist threat.

Member States should:

- Make full use of existing border procedures and systems for security and border management
- Enhance biometric checks and conduct mandatory systematic checks at EU external borders
- Introduce the EES in full and accelerate the preparations for the entry into operation of ETIAS

[54] Commission Staff Working Document on a new approach towards an enhanced and more resilient aviation security policy SWD (2023) 37 final.

[55] Commission implementing regulation (EU) 2025/920 of 19 May 2025; Commission implementing decision (SENSITIVE) of 19 May 2025 – COM (2025) 3014 final.

- Implement recommendations from Schengen evaluation and monitoring mechanism
- Rapidly transpose and implement the CER and NIS2 Directives

2.5 Responding to threats and attacks

Europol and Eurojust offer valuable operational support and expertise to Member States on terrorism investigations and prosecutions. Nevertheless, to ensure a swift and coordinated response to terrorist threats and attacks, the law enforcement and judicial response need to be further strengthened across Europe. In addition, further efforts are needed to close remaining gaps so as to prevent counter terrorist financing. The EU remains committed to not allowing any public money to be used for the promotion of extremism and terrorism.

2.5.1. Countering terrorism financing and financing of violent extremism

The terrorism financing threat is evolving rapidly, benefiting from expanding financing means with crypto assets, digital hawala, and online payment services. At the same time, the global nature of financial services requires a **dynamic European response to terrorist financing**. The EU has put in place a comprehensive framework to prevent money laundering and terrorist financing, with the most recent update in 2024. Member States are urged to transpose the **6th Anti-Money Laundering Directive** by 10 July 2027, in time for the entry into application of the **EU Anti-Money Laundering Regulation**. The **interconnection of bank account registers** by 2029 will further strengthen this framework. Furthermore, since 2010 the **EU-US Terrorist Finance Tracking Program (TFTP) Agreement** allows Member States, Europol and Eurojust to request the U.S. Treasury to search financial messaging data, providing valuable leads to identify terrorists and their financiers.

In order to close existing gaps in tracking terrorist financing, the Commission will launch a study in early 2026 to **assess and identify the measures necessary to establish a future new EU-wide system to enable the retrieval of financial data for the purpose of tracking terrorist financing** and organised crime proceeds. This system should be established by 2030 and aim to cover intra-EU and Single European Payment Area (SEPA) transactions, crypto asset transfers, online and wire payments or transfers.

The **Network of counter-terrorism financial investigators** provides a platform for exchanges on investigations and best practices on a broad range of terrorist financing methods and emerging trends, such as the use of crypto assets, abuse of non-profit organisations and social media platforms, hawala and other informal banking systems. The network builds partnerships with public and private stakeholders and partner countries outside the EU and aims to systematically contributions from the **Europol Financial Intelligence Public Private Partnership.**

The Commission will also support closer **cooperation and information sharing** between financial intelligence units (FIUs), law enforcement, financial institutions, financial technology companies, and online service providers. In particular, tackling **Undesirable Foreign Funding (UFF)**[56] requires closer cooperation between FIUs and intelligence services, building on existing protocols for information exchange. Member States should **ensure that FIUs have the mandate and the capacity to detect and share UFF-related cases**. National Risk

[56] Financial flows from foreign state or non-state actors to natural or legal persons operating in the EU exerting or intending to exert malign influence on European societies by facilitating activities that challenge EU values (Non-legally binding definition used by the EU Knowledge Hub on Prevention of Radicalisation).

Assessments for anti-money laundering and terrorist financing risks should also cover UFF, so FIUs can detect and address them consistently.

The **EU budget must never be misused** to fund projects that promote radical or extremist views. With the revised Financial Regulation[57], the engagement in any wrongful conduct resulting in "incitement to discrimination, hatred or violence" constitutes a clear ground for exclusion from EU funding. The Commission will ensure effective implementation, including by raising awareness, establishing an internal network to exchange information, and by reinforcing processes to take account of information from Member States and other sources where it can be used to assess beneficiaries' and projects' respect for EU values.

Effective protection of the EU budget also relies on Member States actively contributing information to support the Commission's efforts. The outcome of the review of the **Anti-Fraud Architecture** in 2026 will strengthen oversight and accountability to ensure a more efficient protection of the Union's financial interests.

2.5.2. Strengthening the law enforcement response

As announced in the ProtectEU Internal Security Strategy, the Commission will propose an ambitious overhaul of Europol's mandate, which would **reinforce its role as the central information, technological and innovation hub for law enforcement**, to offer stronger support to Member States both on the operational and forensic side.

Subject to the review of Europol's mandate, Europol's European Counter Terrorism Centre (ECTC) should consolidate and further develop operational counter terrorism information for law enforcement in its **central information hub on counter-terrorism**. This hub could also enable real-time information exchange between law enforcement authorities and foster cooperation between law enforcement and the private sector. On the forensic side, the ECTC, together with the Europol Innovation Lab, European Cybercrime Centre (EC3) and other relevant centres, will **enhance operational, analytical and technical support for Member States**. They will build up capacities to process large and complex data sets and develop tools for detecting and disrupting terrorist and extremist online content, as well as terrorist financing.

The Commission will continue to **support European Law Enforcement Networks.**[58] It will also work closely with Member States to update the Council Recommendation on operational law enforcement cooperation[59], to facilitate operational assistance in cross-border scenarios, including moving operational teams and equipment for exercises, not only during crises.

2.5.3. Strengthening judicial cooperation

To counter the terrorist and violent extremist threat in this digital age, lawful access to data for law enforcement and judicial authorities is key. The implementation of the **2025 Roadmap for effective and lawful access to data for law enforcement**[60] will contribute to addressing major challenges standing in the way of successful investigations and prosecutions. The **EU rules on**

---

[57] Article 138 (1)(c)(vi), and Recital 113 of Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast) *OJ L, 2024/2509, 26.9.2024*.

[58] AIRPOL, AQUAPOL, ENLETS, ESG, EIFS, HRSN, RAIPOL and ATLAS.

[59] Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation *OJ L 158, 13.6.2022*.

[60] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Roadmap for lawful and effective access to data for law enforcement COM/2025/349 final.

cross border access to electronic evidence[61] will become applicable in August 2026, allowing judicial authorities to preserve and obtain evidence directly from service providers offering their services in the EU. Building on the **EU-funded SIRIUS project**[62] and the future entry into force of **the UN Convention against Cybercrime** and **the Second Additional Protocol of the Council of Europe Convention on Cybercrime,** international cooperation to obtain electronic evidence will be reinforced through dedicated training and information exchange.

Judicial cooperation and information sharing on terrorism cases is crucial to address the terrorist threat at the prevention and response phases. To facilitate the identification of cross-border links between terrorism cases, Eurojust will upgrade the **European Judicial Counter-Terrorism Register** based on a new state-of-the-art case management system which will be in place before 1 December 2027. Member States are urged to transmit timely information on terrorism cases to Eurojust. The **revision of the Eurojust mandate** will help reinforce its analysis capacity and enable closer cooperation with Europol, strengthening support to cross-border terrorism investigations and prosecutions. Moreover, the 2016 Procedural Safeguards Directive for children[63] will continue to offer targeted support and protection measures for children entering the criminal justice system. **Battlefield evidence** is essential to prosecute returning foreign terrorist fighters. Data derived from battlefield evidence, once inserted into the SIS, also helps detect foreign terrorist fighters at EU borders. The end of the United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ISIL (UNITAD) limits the availability of battlefield evidence. The Commission, together with Eurojust, will explore whether and how information collected by **the Iraqi authorities and UNITAD** could be made accessible to Member States through enhanced cooperation between **Eurojust** and the **National Centre for International Judicial Cooperation of Iraq** and whether information linked to individual cases could be stored in **Eurojust's Core International Crime Database**.

KEY ACTIONS

The Commission will:

- Assess and identify the measures necessary to establish an EU Financial data Retrieval System for the purpose of tracking terrorist financing and organised crime proceeds
- Strengthen the system protecting the EU budget from misuse, including through the review of the EU's Anti-Fraud Architecture
- Propose revisions of the mandates of Europol and Eurojust, strengthening their roles in law enforcement and judicial response to terrorism

The Commission, together with Member States and Europol, will:

- Strengthen cooperation and information sharing between financial intelligence units (FIUs), law enforcement, financial institutions, financial technology companies, online service providers and social media platforms
- Implement the actions in the Roadmap on lawful and effective access to data for law enforcement

Europol will:

- Consolidate and further develop its central information hub on counter-terrorism

[61] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings *OJ L 191, 28.7.2023*.

[62] EU-funded SIRIUS project serves as a go-to point for obtaining electronic data from service providers based in other jurisdictions for over 8000 members from 47 jurisdictions.

[63] Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings *OJ L 132, 21.5.2016*

- Enhance operational, analytical and technical support for Member States' law enforcement counter-terrorism efforts

Together with the Commission, Eurojust will:

- Explore ways of making information collected by UNITAD and the Iraqi authorities accessible to Member States

2.6 Cooperating with international partners

The external and internal dimensions of terrorism and violent extremism are intrinsically linked[64]. The Commission, working with the High Representative and the EU Counter-Terrorism Coordinator, will strengthen international cooperation across all pillars of this Agenda, following a human-rights based approach.

2.6.1. Restrictive measures on terrorism

The listing of individuals, groups and entities under EU restrictive measures to combat terrorism[65] ('EU Terrorist List') remains a vital tool to disrupt terrorist networks. The EU Terrorist List should be continuously updated to reflect and address evolving threats, by disrupting financial flows and preventing support for terrorist activities. The High Representative and EU Member States are **assessing how to make the EU Terrorist List more effective, operational and agile**. The expansion of the scope of the regime and closer cooperation with like-minded third countries will contribute to its functionality.

2.6.2. Advancing international agreements

The Commission will propose to sign and conclude on behalf of the EU the **new Protocol amending the definition of terrorist offences** in the Council of Europe Convention on the prevention of terrorism. Once in force, the framework will provide a **common pan-European definition of terrorist offences** for more than 40 countries.

The Commission aims to further **strengthen Europol and Eurojust's external cooperation** on counter-terrorism through international agreements on the exchange of personal data with third countries and international organisations, with a focus on key regions.

2.6.3. Deepening bilateral and regional cooperation

Cooperation with **enlargement partners** will be strengthened to facilitate their accelerated integration into the EU's security architecture and promote the alignment of their legal and strategic frameworks with the EU *acquis* and standards. Wherever possible, they will be **gradually integrated into EU actions** such as the Knowledge Hub on the prevention of radicalisation and activities of Europol, Eurojust and CEPOL, and will benefit from the tools, guidance and capacity-building provided to Member States.

The new **Joint Action Plan on preventing and countering terrorism and violent extremism for the Western Balkans 2025-2030** also supports their alignment with the EU acquis, advances operational cooperation, and enhances capacities of our partners in the region. Candidate countries and potential candidates will further benefit from dedicated technical assistance, capacity building and EU financing of projects, for instance on protection of public spaces and critical infrastructure or border management.

---

[64] Council Conclusions on reinforcing external-internal connections in the fight against terrorism and violent extremism of 16 December 2024.

[65] Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP) *OJ L 344, 28.12.2001*.

The **Middle East and North Africa** hold a strategic place in the global fight against terrorism. Under the **Pact for the Mediterranean**, EU support will focus on strengthening border management, enhancing law enforcement and judicial cooperation and preventing violent extremism and terrorism, with the support of the Knowledge Hub on the prevention of radicalisation. A regional dialogue on internal security will contribute to combatting serious and organised crime and terrorism.

The EU will continue to support the recovery of **Syria** supporting a peaceful and inclusive transition and reconciliation within Syria, as well as its regional reintegration. In addition, the EU will provide a financial support package of around €620 million for 2026 and 2027, including humanitarian aid, early recovery support and bilateral support, while continuing crisis response efforts in Northeast Syria and the camps. The Commission also encourages EU institutions and Member States to implement the Council Conclusions of 23 June 2025 on Syria, as well as the recommendations of the **Action Plan on countering the terrorism threat emanating from Syria** issued by the EU Counter-Terrorism Coordinator.

In **Africa**, notably in Sub-Saharan Africa, various terrorist groups are gaining power. The situation in **Central and South Asia**, with mounting regional tensions and expanding influence of ISKP, also necessitates close monitoring. The EU will reinforce its integrated response by **embedding security considerations in the 360 approach of the Global Gateway** and **strengthening direct support for capacity-building**. Programmes will reinforce border security, support operational cooperation, strengthen capacities to detect and disrupt illicit financial flows, address extremist and violent propaganda, tackle misuse of new technologies and the expanding terrorism-organised crime nexus in several regions, build community resilience against radicalisation and recruitment into terrorist groups, and facilitate rehabilitation and reintegration of former fighters and families.

Coordination of the EU and Member States' external action in third countries is particularly important to avoid duplications. The Commission, together with Member States, will regularly map projects funded by the EU and by Member States, cultivate new Team Europe initiatives, and foster synergies between EU action and Common Security and Defence Policy missions and operations in countries particularly affected by terrorism.

Counter-terrorism dialogues facilitate strategic exchanges with third countries and should lead to clear and actionable conclusions that are effectively implemented. The **EU Counter-Terrorism Experts Network** is key to sharing information on the security situation in third countries. The High Representative will work to strengthen the Network, ensuring broader regional coverage and closer cooperation, addressing the terrorism-organised crime nexus, terrorist financing and propaganda.

2.6.4. Reinforcing the EU's role on the multilateral stage

The High Representative, the Commission and the EU Counter Terrorism Coordinator will ensure **close EU coordination and stronger EU leadership in multilateral fora.** The EU will continue to leverage its co-chairmanship of the Global Counter Terrorism Forum (GCTF) to advance civilian-led counter-terrorism action and promote sustainable and coordinated multilateral efforts.

The EU will also use its role within the Global Coalition Against Da'esh to strengthen coordination in the region. The EU, alongside Member States, will play an important role in the **review of the UN Global Counter Terrorism Strategy** in 2026 to promote EU values and priorities, and will continue to contribute to the **ongoing reform process of the UN,** the UN80 initiative, which includes the UN's **counter-terrorism architecture**.

Engagement with the **Council of Europe,** the **Financial Action Task Force (FATF), Interpol and NATO** will be maintained on a thematic basis. By collaborating with fora such as the Financial Action Task Force and the Global Counter Terrorism Forum, the EU will also address the interconnected challenges posed by terrorist financing, recruitment, and propaganda, especially on social media. The **Global Internet Forum to Counter Terrorism (GIFCT)** will also remain a key partner for the Commission. And finally, the Commission will continue its engagement in the **Christchurch Call Foundation**[66].

KEY ACTIONS

The Commission will:

- Propose to sign and conclude the Protocol amending the definition of terrorist offences in the Council of Europe Convention on the prevention of terrorism
- Recommend to the Council to authorise the Commission to negotiate international agreements with further third countries on cooperation with Eurojust and Europol
- Support the implementation of the Joint Action Plan on preventing and countering terrorism and violent extremism for the Western Balkans 2025-2030
- Extend the activities of the Knowledge Hub to EU candidate countries and the Mediterranean region
- Embed security considerations in programmes under the Global Gateway Strategy and strengthen direct support for capacity building

The Commission, together with EU Member States, will:

- Regularly map counter-terrorism and preventing and countering violent extremism (CT/PCVE) projects funded by the EU and Member States

The High Representative will:

- Together with the Commission, the EU Counter Terrorism Coordinator and Member States, further operationalise Counter-Terrorism dialogues
- Strengthen the EU Counter Terrorism Experts Network
- Together with the Commission and the EU Counter Terrorism Coordinator, ensure close EU coordination and strong EU leadership in multilateral fora

The High Representative and the Council should:

- Regularly review the Common Position 2001/931/CFSP ('EU Terrorist List')

3. Conclusion

Terrorism and violent extremism continue to be a challenge to Europe's security. This Agenda sets out the EU response: a collective commitment to face these threats with foresight, unity and resolve. It gives direction to all our efforts: **prevention before violence takes root, protection where people are most vulnerable, and justice against those who seek harm.**

Through this Agenda, the European Union will sharpen its collective capacity to anticipate threats, to prevent radicalisation, protect its people both online and offline, and to respond firmly when attacks occur, streamlining this approach within and beyond its borders. The

[66] The Christchurch Call Foundation is a non-governmental organisation initiated by New Zealand and France in response to the horrific terrorist attack in Christchurch in 2019 to eliminate terrorist and violent extremist content online.

Agenda will deliver ambitious action across all pillars, giving priority to **several initiatives** that address emerging challenges, such as:

- **a prevention toolbox to counter the radicalisation of minors;**
- **a potential strengthening of the Terrorist Content Online Regulation;**
- **a 'post-hit' procedure to share hit information on terrorism-related alerts in the Schengen Information System; and**
- **a new EU Financial data Retrieval System.**

The Commission will drive delivery across all pillars, track implementation, and ensure that the Union's instruments, legislation and funding are used to their full potential. The Commission will inform and involve the European Parliament, the Council, the EU Counter Terrorism Coordinator, Member States, the private sector and civil society in delivering this Agenda.