Terrorism – Studies, Analyses, Prevention, 2026, no. 9: 263–283

https://doi.org/10.4467/27204383TER.26.012.23795

Article

Digital revolution of the EU's counter-terrorism policy under the new EU Agenda for Combating Terrorism of 2026

PIOTR BURCZANIUK

https://orcid.org/0000-0002-6685-8769

Institute of Legal Sciences,
Cardinal Stefan Wyszyński University

Abstract

On 26 February 2026, the European Commission published a new European Union Agenda for Preventing and Combating Terrorism in the form of communication, replacing a similar document that had been in force since 9 December 2020. The need to implement the new European Internal Security Strategy 'Protect EU' adopted on 1 April 2025 was cited as the main reason for the changes. The primary objective of the study is to outline the content of the new Agenda, with particular attention to the new approach presented therein regarding terrorist threats and violent extremism. The approach is gradually shifting away from traditional, physical terrorist threats in favour of threats that take a hybrid form or occur exclusively in the digital environment. The analysis of the document focuses on presenting the new map of terrorist threats outlined therein, based on six pillars encompassing: anticipating threats, preventing radicalisation, protecting citizens online, protecting citizens in the physical environment, responding to threats and attacks, as well as cooperation with international partners. The article pays particular attention

to the issue of the Agenda's place within the system of European legal sources and the normative effect that arises from it. The most significant differences in the approach to combating terrorism and violent extremism in the old and new agendas were also outlined.

Keywords

terrorism, violent extremism, EU security policy, EU Agenda 2026, ProtectEU, digitalisation of security, new technologies in the fight against terrorism

Agenda to combat terrorism as part of the ProtectEU strategy

On 26 February 2026, the European Commission (hereinafter: Commission or EC) published the new European Union agenda entitled *ProtectEU: Agenda to prevent and counter terrorism* (hereinafter: Agenda)[1] in the form of the communication addressed to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. It replaced the previous agenda entitled *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*, published by the EC on 9 December 2020[2].

The main aim of the article is to provide a critical analysis of the assumptions underlying the Agenda and to demonstrate how it redefines EU's internal security policy by shifting the focus from the traditional (physical) countering of terrorism to addressing hybrid and digital threats. The main research problem of the article can be formulated as the following question: how have digitalisation, the development of new technologies, and changes in the geopolitical environment influenced

[1] *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*, COM(2026) 101 final of 26 February 2026, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52026DC0101 [accessed: 28 IV 2026].

[2] *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, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0795 [accessed: 28 IV 2026].

the evolution of EU's counterterrorism policy, and do the solutions adopted in the Agenda signify a lasting transition of the EU from a reactive-operational model to a technology-driven preventive model?

The article combines several research approaches. The study draws primarily on: the dogmatic-legal method, which was used for exegesis of the primary and secondary legislation of the EU and the case law of the Court of Justice of the European Union; the comparative method, used in the conclusion of the article, and the systemic-institutional method, applied to describe the EU's security architecture.

Work on the Agenda was initiated by the EC as part of the implementation of the ProtectEU: a European Internal Security Strategy, published on 1 April 2025 (hereinafter: Strategy)[3]. It constitutes a comprehensive update of the EU's approach to internal security and is based on the premise that protecting citizens and ensuring the stability of the EU's internal environment require integrated and multi-level action by all stakeholders, including EU institutions, Member States, national security and intelligence services, the private sector, and civil society.

The key element of the Strategy is to strengthen the EU's capacity to anticipate threats through the development of risk analyses, better exchange of information and the use of data provided by the EU agencies, particularly Europol. The Strategy emphasises prevention and combating of threats, particularly terrorism, organised crime and cybercrime, by dismantling criminal networks, preventing radicalisation, particularly online and restricting the sources of funding for criminal activities. Critical infrastructure security is also a significant pillar of the Strategy, which is intended to make the EU more resilient to sabotage, hybrid attacks and technological disruptions. Considerable importance is attached to strengthening the cybersecurity and resilience of digital systems, which are increasingly becoming a target of criminal and destabilising activities. The Strategy emphasises that:

> (...) the terrorist threat level in Europe continues to loom. Regional crises outside the EU create a ripple effect, providing new motivation for terrorist actors across the entire ideological spectrum to recruit,

[3] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy*, COM(2025) 148 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52025DC0148 [accessed: 28 IV 2026].

> mobilise or build up their capacities. They target their radicalisation and recruitment efforts specifically towards the most vulnerable sections of our societies and in particular certain young people. They inspire lone actor attacks and a surge in anti-system extremism whose goal is to disrupt the democratic legal order[4].

The fight against terrorism and violent extremism is becoming one of the pillars of the Strategy. The whole of section 6 is devoted to this issue. It is envisaged that a comprehensive counter-terrorism plan will be introduced to prevent radicalisation, secure the online and public spaces, curb funding channels, and respond to attacks should they occur.

The Strategy, similarly to the Agenda, does not define the term terrorism. Instead, it refers to the definition of 'terrorist offence' within the meaning of Article 3 of the *Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA*. According to that definition, these are (...) *offences, which, given their nature or context, may seriously damage a country or an international organisation,* if they are committed intentionally and for so-called terrorist purposes. Such damage includes:

a) seriously intimidating a population,
b) unduly compelling a government or an international organisation to perform or abstain from performing any act,
c) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a state or an international organisation.

At the same time, it should be noted that no legal definition of violent extremism has been adopted in the EU legislation. The Agenda merely states in a footnote that (...) *violent extremist acts do not meet the threshold set by the definition of terrorist offences; however, they pose a serious threat to security*[5].

In the Strategy, the EC identified the following as the four key elements of the fight against terrorism:

---

[4] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy...*, point 1.

[5] *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) prevention of radicalisation and protection of people online – the Commission recognises the need to tackle the root causes and, above all, highlights the way in which terrorists and violent extremists use online platforms to disseminate (particularly among minors) terrorist and other harmful content, to raise funds and to recruit. A key role in combating the spread of terrorist content online plays the *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online*, as it enables the rapid removal of the most repulsive and dangerous materials;
2) counter terrorism financing – the Commission points out that terrorists raise funds for their operations through crowdfunding campaigns, crypto-assets, neobanks or online payment platforms. Law enforcement authorities must detect and investigate these financial flows, which requires appropriate resources, tools and specialist knowledge;
3) protection from attacks – in addition to investing in preventing radicalisation, an important element of protecting citizens is limiting the means by which terrorists and criminals can carry out attacks. Action is needed both in relation to the tools used by terrorists and the protection of targets at risk of attack, with particular attention paid to public spaces. The Commission also points to the increasing security threats caused by the use of unmanned aerial vehicles for espionage and attacks;
4) foreign terrorist fighters – the Commission, together with Europol, has set out to strengthen cooperation with key third countries in order to obtain biographic and biometric data on individuals that might pose a terrorist threat, including foreign terrorist fighters. This data is to be entered into the Schengen Information System (SIS). The Commission emphasises how important it is for Member States to make use of all existing tools, including the SIS, as well as to improve biometric checks and carry out mandatory and systematic checks on all persons at the EU's external borders.

One of the most important measures in combating terrorism and violent extremism envisaged in the Strategy was the adoption in 2025 of a new EU Agenda in order to prevent and counter terrorism and violent extremism. The Agenda was ultimately adopted on 26 February 2026.

The place of the Agenda in the EU legal framework

The legal basis for the EU's actions to prevent and combat terrorism is provided by the provisions of the Treaty on the Functioning of the European Union (hereinafter: TFEU). As part of the regulation of the area of freedom, security and justice (title V), Article 67(3) of the TFEU sets out the EU's obligation to make every (...) *endeavour to ensure a high level of security through measures to prevent and combat crime, racism and xenophobia, and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments in criminal matters and, if necessary, through the approximation of criminal laws*.

Article 83 of the TFEU constitutes the principal means of achieving this objective. It empowers the European Parliament and the Council by means of directives to (...) *establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis*. The TFEU classifies the following as areas of this crime: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime.

In addition, in accordance with Article 84 of the TFEU: *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may establish measures to promote and support the action of Member States in the field of crime prevention, excluding any harmonisation of the laws and regulations of the Member States*. It is on this basis that the European Parliament and the Council may adopt strategy and agenda documents which set policy directions but are not directly binding in nature. At the same time, Article 17 of the Treaty on European Union (hereinafter: TEU) assigns the EC the task of supporting the general interest of the EU and, to that end, taking appropriate initiatives.

In summary, the adoption of strategies such as Agenda is not based on a single specific legal basis, but rather on a set of Treaty provisions. These provisions:

- set out the objective of the EU aimed at ensuring security (Article 67 of the TFEU),
- grant the EU powers to combat terrorism (Article 83 of the TFEU),
- enable supportive and strategic actions (Article 84 of the TFEU),

– give the Commission the role of driving EU policies (Article 17 of the TEU).

It is also worth noting that, in accordance with Article 4(2), third sentence of the TEU: (...) *In particular, national security remains the sole responsibility of each Member State*. This means that the EU's actions – including anti-terrorist strategies – are purely of a coordinating and supportive nature and do not replace national policies.

On these legal ground, the EC may accept strategic documents in the form of, among others, COM documents. They include official positions, strategies, analyses and announcements of legislative actions of the Commission and play a role of the so-called soft law. The role and the importance of such a law results mainly from the case law of the Court of Justice of the EU (CJEU). It emphasises that such law has no binding force, but cannot be completely ignored when interpreting EU law[6]. It may be a point of reference for interpretation, especially when it clarifies EU policy[7], and at the same time it binds the Commission in its own practice, although it is not formally binding on the Member States of the EU[8].

Map of terrorist threats according to the Agenda

The Agenda begins with an introduction in which the EC analyses the most significant risks and emphasises that (...) *terrorism and violent extremism 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*[9].

[6] Cf. Judgment of the Court (Second Chamber) of 13 XII 1989 Salvatore Grimaldi v Fonds des maladies professionnelles. ECLI: EU:C:1989:646.

[7] Cf. Opinion of Advocate General Van Gerven delivered on 15 October 1992. ECLI: EU:C:1992:393.

[8] Cf. Joined Cases C-189/02 P, C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P. Dansk Rørindustri and Others v Commission of the European Communities.

[9] *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...*, p. 1.

As the authors of this document point out, the number of coordinated and large-scale attacks in the EU has decreased in recent years, however the threat has not disappeared, but has evolved, both subjectively and ideologically. The number of perpetrators acting alone and in small groups of several people, whose core is often minors, is growing. In terms of ideological motivation, it is emphasised that (...) *while jihadist terrorism remains the most prominent and lethal terrorist threat, 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*[10].

Furthermore, the EC notes that security in the EU, including the terrorist threat level, is influenced by the changing geopolitical environment and external conflicts affecting the EU, primarily in the Gaza Strip, as well as – in the context of an increase in the number of acts of sabotage and hybrid operations – the ongoing Russian war of aggression against Ukraine. The European Union faced complex threats stemming from both terrorist groups as well as foreign state and non-state actors. These entities model their actions on those traditionally attributed to terrorist groups, e.g. they use improvised ignition devices in aerial munitions, they carry out cyber attacks or sabotage of critical infrastructure, but also use terrorists and violent extremists as supporters. Links are formed and maintained between terrorism, organised crime and cybercrime. They utilise criminal service models and shared resources, primarily in the areas of recruitment, criminal trading platforms and underground banking networks.

Significant part of contemporary terrorism is its strong connection to the digital environment. Internet, social media, online gaming platforms have become key tools used by extremist organisations and individuals holding such views to conduct propaganda, recruit new members, as well as to exchange information and plan activities. The Agenda states that:

> 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'[11]. Generative AI is abused to create instruction

[10] Ibid.

[11] Digital hawala is informal system for transferring financial value through the use of digital tools, operating outside the traditional banking system and relying on a network of trusted intermediaries.

> 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[12].

The Commission indicates that described threats are cross-border in nature. This means that no Member State is able to counter them effectively on its own. Therefore, it is necessary to strengthen the cooperation at EU and international level. However, it should not be forgotten, as the Commission emphasises, that a balance must be struck between ensuring security and protecting fundamental rights. Antiterrorist actions must be taken in accordance with EU values, such as democracy, the rule of law and respect for human rights. It is important in terms of both the legality of the actions taken and for maintaining public confidence in them.

Six pillars of the fight against terrorism and violent extremism

In the second point of the Agenda, the Commission sets out a comprehensive approach to counter terrorism and violent extremism based on a system of six interlinked pillars of action. These are: 1) anticipating threats, 2) preventing radicalisation, 3) protecting people online, 4) protecting people in the physical environment, 5) responding to threats and attacks, 6) cooperating with international partners. This approach reflects the belief that an effective antiterrorist policy cannot be limited to reacting to events, but must encompass the full spectrum of measures – from identifying risks, to prevention, as well as response and recovery following any attacks. Contemporary threats are dynamic, multidimensional and often cross-border, which requires an integrated approach involving various levels of government – local, national, EU and international.

Anticipating threats

The Commission highlights that (...) *security starts with effective anticipation and foresight*[13].

[12] *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...*, p. 3.

[13] Ibid, p. 4.

Anticipating threats is intended to form the foundation of the entire strategy and be based on the gathering, analysis and exchange of information. Cooperation between Member States and EU agencies, including the Single Intelligence Analysis Capacity[14], which provides timely risk assessments, and Europol, which draws up regular reports on trends based on information received from law enforcement authorities, plays a key role in this regard. Dynamic and unpredictable nature of emerging threats requires – according to the Commission – strengthening the ability of law enforcement agencies to anticipate, in order to better identify emerging threats and take appropriate actions to combat terrorism.

In turn, anticipating is crucial from the perspective of identifying threats and is to be based on two elements. The first of these is to use the potential of new technologies in law enforcement. Artificial intelligence (AI), machine learning or big data analysis is a tool-based potential that allows for the identification of behavioural patterns and the detection of warning signals that may indicate the preparation of attacks. The second element is to prepare to counter the use by terrorists of new technology, such as AI, online platforms, electronic financing methods, particularly crypto-assets, or the use of 3D-printed weapons. Forecasting activities are to be based on the work of the Joint Research Centre of the European Commission and their financing basis is to be the Horizon Europe programme.

Analysis of the principles underlying this pillar leads to the conclusion that there should be a shift from reactive model previously presented by the EU to a preventive model, in which action is taken before the threat materialises.

Preventing radicalisation

The Commission defines preventing radicalisation as (...) *tackling its drivers before they take root*[15]. The second pillar is based on four elements:

[14] SIAC – a structure linking the civilian EU INTCEN (European Union Intelligence and Situation Centre), i.e. the EU civilian intelligence unit, which is part of the European External Action Service with Military Intelligence Directorate as part of the European Union Military Staff (EUMS).

[15] *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...*, p. 5.

1) developing a prevention toolbox for minors. These tools are intended to enable early detection, strengthen protective factors, build resilience through education and social integration, in particular of minors, as well as support families and communities in using the internet safely;
2) building resilient societies, with a view to protecting all religious communities from hatred, discrimination and violence. The work of the EC will focus on using AI to improve detection of extremist content, develop common threat indicators and streamline cooperation between platforms, law enforcements agencies and scientists in order to identify propaganda generated by AI and coordinated campaigns aimed at radicalisation;
3) addressing radicalisation in prisons, prison leavers and managing the return of Foreign Terrorist Fighters and their family members. The basis is to develop tools for risk assessment and management in the pre-release phase and guidelines supporting national approaches to radicalised prison leavers and returnees, combined with training in rehabilitation and reintegration, with particular emphasis on the protection of children;
4) supporting victims of terrorism by raising awareness of the EU Remembrance Day for victims of terrorism and supporting victims' associations by promoting their active role in prevention programmes.

Institutionally, activities within the second pillar are handled by the EU Knowledge Hub on Prevention of Radicalisation established in 2024. The Centre draws up guidelines, tools, training and support services for decision-makers and practitioners.

Protecting people online

The European Union adopted the world's most advanced regulatory framework for combating terrorist activity online, but the threat continues to evolve. The Agenda states that: *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*[16].

[16] Ibid, p. 8.

According to the Commission's guidelines, activities in this pillar are to focus on three issues:

1) making full use of regulatory frameworks to tackle terrorist and extremist content online by, among others, development by Europol of European hash-sharing database, i.e. database of digital traces for terrorist and violent extremist content, which will enable Member States and hosting service providers to securely flag, match and remove content across various platforms;
2) working with industry, mainly with online service providers, which will be implemented through the EU Internet Forum (which brings together EU Member States' ministries, law enforcement authorities, civil society and online service providers, including social media platforms) and by activities together with the European Board for Digital Services to intensify the fight against the dissemination of terrorist and violent extremist content;
3) ensuring effective and coordinated crisis response online, assuming the transformation of the existing EU Crisis Protocol into an EU Online Crisis Response Framework (included in the Digital Services Act). Member States will be able to use it where an incident leads to heightened online activity related to an attack.

Protecting people in the physical environment

The fourth pillar is based on changed approach, according to which the foundation is action based on resilience. It replaced the action focused on security. This occurred with the adoption in 2022 of the *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* (hereinafter: CER Directive). At the same time, the EU provides practical support based on EU security advisors. Their task is to assist in assessing vulnerability to threats and suggesting specific improvements. According to the Agenda, EU activities in the pillar under review are to focus on five issues:

1) impeding terrorist travel, by ensuring a high level of protection of the EU external borders. This is primarily achieved through large-scale information systems: the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS), the Visa Information System (VIS) and the interoperability framework. The big challenges remain cooperation with third

countries to obtain biographic and biometric data on individuals that might pose a terrorist threat and entering this data into the SIS system, as well as developing the procedure to be followed in the event of a 'hit'. The so-called screening process is due to come into application in June 2026[17]. Thanks to it, 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 is set to become easier. The Commission emphasises that it will promote the efficient return of individuals posing a security risk;

2) restricting access to means used to carry out attacks by harmonisation regulations on the criminalisation of illegal firearms trafficking and other firearms-related offences, including the illicit creation, possession and dissemination of blueprints to manufacture 3-D printed firearms. The Agenda also assumes a review of the *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* and the presentation of a new action plan for preparedness and response to chemical, biological, radiological and nuclear (CBRN) risks in 2026;
3) addressing the threat posed by drones. The Commission emphasises the importance of the threat associated with the use of new and emerging technologies, particularly drones by terrorist actors. Counter-drone operations are to be based on the Drone Strategy 2.0[18] and the EU Action Plan on Drone and Counter Drone Strategy presented on 11 February 2026[19];
4) protecting public spaces in Europe, whereas it is necessary to take into account security requirements already at the design stage

[17] *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 and amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817*.

[18] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 'A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe'*, COM(2022) 652 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0652 [accessed: 28 IV 2026].

[19] *Action Plan on Drone and Counter Drone Strategy*, European Commission, https://digital-strategy.ec.europa.eu/en/policies/drone-security [accessed: 28 IV 2026].

of urban areas, public spaces and places of worship. This should be reflected in appropriate obligations for operators of public spaces to implement security measures based on risk assessments. In organisational terms, this task is entrusted to the reinforced EU Forum on the Protection of Public Spaces;

5) resilience of critical entities, transport and supply chain security. This is linked to growing concerns about possible incidents in the form of hybrid campaigns and acts of sabotage by hostile state actors and their proxies. In order to improve security, the EC recommends urgent implementation of the aforementioned CER Directive and the *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)*.

Responding to threats and attacks

The fifth pillar is to be based on a rapid and coordinated response provided by the law enforcement and judicial authorities, which require reinforcement, with the support of Europol and Eurojust. The Commission also highlights the need to take further actions aimed at eliminating gaps in the system for preventing the financing of terrorism.

Activities within this pillar are to focus on three issues:

1) countering terrorism financing and financing of violent extremism. The Commission highlights that the global nature of financial services requires the active response of the whole of Europe to the issue of terrorist financing. This is also of significant importance because of new sources of financing, such as crypto assets, digital hawala (and online payment services). The Commission considers the full implementation of the EU package on *anti-money laundering and countering the financing of terrorism* (AML/CFT), adopted on 30 May 2024, as the legal foundation for combating the financing of terrorism. The package includes the *Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing* (it will come into force on 10 July 2027) and the *Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on*

the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849. The Commission also plans to begin work on developing a EU-wide system that will enable the retrieval of financial data in order to track funds belonging to terrorists and organised crime proceeds. The system is due to be established by 2030 and will include intra-EU and Single European Payment Area (SEPA) transactions, crypto asset transfers, online payments or electronic fund transfers;

2) strengthening the law enforcement authorities response through enhancing the Europol's mandate, mainly its European Counter Terrorism Centre (ECTC) as a leading centre for information, technology and innovation for the law enforcement;
3) strengthening judicial cooperation through full implementation of the *Roadmap for lawful and effective access to data for law enforcement* [20] adopted by the Communication from the Commission of 24 June 2025. The ability to secure and obtain evidence directly from service providers offering their services in the EU is of crucial importance, pursuant to the *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*, which has been in force since 18 August 2026. The Commission draws attention to the essence of the SIRIUS project, endorsed by the EU, which is an EU system designed to support law enforcement authorities in gathering evidence from the internet across national borders[21].

[20] *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, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0349 [accessed: 29 IV 2026].

[21] *SIRIUS project*, Europol, 21 I 2026, https://www.europol.europa.eu/how-we-work/sirius-project [accessed: 29 IV 2026].

Cooperating with international partners

The last pillar implies the need to strengthen international cooperation, primarily through the activities of the High Representative and the EU Counter-Terrorism Coordinator.

Activities under this pillar are to focus on four issues:

1) restrictive measures to combat terrorism, with the EU Terrorist List serving as the main tool to disrupt terrorist networks[22];
2) advancing international agreements, where the biggest challenge remains new Protocol amending the definition of terrorist offences in the Council of Europe Convention on the prevention of terrorism[23]. Once it comes into force, it is intended to provide a common pan-European definition of terrorist offences for more than 40 countries;
3) deepening bilateral and regional cooperation, in particular strengthening cooperation with partners involved in the EU enlargement process, as well as on measures targeting specific regions, with particular attention being paid to the Western Balkans, the Middle East, including Syria, as well as African countries;
4) reinforcing the EU's role by coordination and activities within the multilateral forums of the High Representative, the Commission and the EU Counter Terrorism Coordinator. Thematic cooperation with the Council of Europe, the Financial Action Task Force, Interpol and NATO is to be maintained.

The 2026 vs. 2020 Agenda

The 2026 Agenda, which was drafted with a view to implementing the new ProtectEU Internal Security Strategy published on 1 April 2025, makes the adoption of the EU's strategy for combating terrorism and violent

[22] The official list of individuals, groups, and entities designated by the EU as involved in terrorist activities is formally maintained pursuant to the *Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP)*.

[23] Council of Europe Committee on Counter-Terrorism (CDCT) – Draft Protocol amending the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196), https://search.coe.int/cm/g#{%22CoEIdentifier%22:[%220912594880264105%22],%22sort%22:[%22CoEValidationDate%20Descending%22]} [accessed: 14 V 2026].

extremism to current threats a central theme. As the Commission points out, their nature has undergone a noticeable shift – from traditional, physical terrorist threats to threats that take on a hybrid form or exist only in digital environment. Reactive-operational approach is therefore replaced by an approach focused on proactive, systemic actions in the digital sphere.

The 2020 Agenda addressed terrorist threats in the traditional way, as activities carried out by organised groups that were ideologically motivated and conducted primarily 'offline'. Internet appeared in it only as one of the tools and did not constitute the central focus of interest. The new Agenda considers digital space to be the primary environment in which threats occur. Radicalisation, recruitment, propaganda and financing are increasingly taking place exclusively in a virtual environment, which means that threats are more scattered, harder to detect at an early stage, and strongly linked to disinformation and information manipulation. The Agenda implies the need to shift from the approach focused on combating a specific organisation to one centred on managing a dynamic, primarily digital ecosystem of threats.

The approach to carrying out preventive measures has also changed. The previous Agenda was focused on countering radicalisation, including through social programmes, monitoring of high-risk groups and cooperation of the services. In 2026 Agenda, prevention is largely shifting online, with a focus on the early detection of extremist content, countering its algorithmic amplification, its rapid removal and limiting its reach. In this way, prrevention is becoming more technology-driven and automated, and relies less on social activities.

In the previous Agenda, digital technologies were the tool only supporting activities (e.g. data analyses, information exchange). In the new Agenda technologies are becoming a central element of the strategy, focused primarily on using AI to identify threats, analyse big data, automate security processes and develop predictive tools. The difference, therefore, lies in the shift from a level of technological support to a strategy based on technology.

Both documents emphasise the importance of cooperation, however, the previous Agenda focused exclusively on the cooperation between Member States and EU agencies, while the new one has expanded this to include private sector, technological entities and global cooperation. This cooperation is becoming networked and multi-layered. In the 2020 document, private sector (particularly online platforms) acted as a partner

supporting the activities of states. In the 2026 Agenda, the role of this sector is clearly expanded. Social platforms are becoming jointly responsible for security. The Commission expects them to actively detect and remove content as well as to put in place systemic cooperation and monitoring mechanisms. There is a shift from the model of voluntary cooperation towards the model of shared regulatory responsibility.

There is also a noticeable shift in the approach to building public resilience. In 2020 Strategy, this resilience was important but was treated more as a supplementary element. In the new Agenda, it has become one of the most important pillars, primarily in the fight against disinformation, building digital awareness, and reducing online vulnerability to radicalisation. Security no longer concerns just a specific institution, but society as a whole, as a system.

In summary, it is important to remember that the adopted Agenda is, in fact, a document of a purely programme-related nature. The implementation of its objectives is to be achieved through proposed or already implemented EU legislative acts and activities focused mainly on developing cooperation among the law enforcement authorities of EU Member States and third countries, under the coordination of organisationally strengthened Europol with actual executive functions.

Bibliography

Internet sources

Action Plan on Drone and Counter Drone Strategy, European Commission, https://digital-strategy.ec.europa.eu/en/policies/drone-security [accessed: 28 IV 2026].

SIRIUS project, Europol, 21 I 2026, https://www.europol.europa.eu/how-we-work/sirius-project [accessed: 29 IV 2026].

Legal acts

Treaty on the Functioning of the European Union (Journal of Laws of 2004, no. 90, item 864).

Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Official Journal of the EU L 1624 of 19 VI 2024).

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 and amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817 (Official Journal of the EU L 1356 of 22 V 2024).

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 (Official Journal of the EU L 191/118 of 28 VII 2023).

Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Official Journal of the EU L 172/79 of 17 V 2021).

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 (Official Journal of the EU L 186/1 of 11 VII 2019).

Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 (Official Journal of the EU L 1640 of 19 VI 2024).

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 (Official Journal of the EU L 333/164 of 27 XII 2022).

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) – (Official Journal of the EU L 333/80 of 27 XII 2016).

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (Official Journal of the EU L 88/6 of 31 III 2017).

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, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0795 [accessed: 28 IV 2026].

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, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0349 [accessed: 29 IV 2026].

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, COM(2026) 101 final of 26 February 2026, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52026DC0101 [accessed: 28 IV 2026].

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 'A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe', COM(2022) 652 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0652 [accessed: 28 IV 2026].

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy, COM(2025) 148 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0148 [accessed: 28 IV 2026].

Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP) – (Official Journal of the EU L 344/93 of 28 XII 2001).

Case law

Judgment of the Court (Second Chamber) of 13 XII 1989 Salvatore Grimaldi v Fonds des maladies professionnelles. ECLI: EU:C:1989:646.

Opinion of Advocate General Van Gerven delivered on 15 October 1992. ECLI: EU:C:1992:393.

Joined Cases C-189/02 P C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P. Dansk Rørindustri and Others v Commission of the European Communities. ECLI: EU:C:2005:408.

Other documents

Council of Europe Committee on Counter-Terrorism (CDCT) – Draft Protocol amending the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196), https://search.coe.int/cm/eng#{%22CoEIdentifier%22:[%220912594880264105%22],%22sort%22:[%22CoEValidationDate%20Descending%22]} [accessed: 14 V 2026].

Piotr Burczaniuk, PhD

Doctor of Law, Assistant Professor at the Chair of the Theory and Philosophy of Law of the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw; legal counsel, member of the Regional Chamber of Legal Advisers in Warsaw; legislator, member of the Polish Legislation Society; legislative expert. Author of publications on the theory and philosophy of law, constitutional law and economic law.

Contact: p.burczaniuk@uksw.edu.pl