



**Brussels, 11 September 2026
(OR. en)**

13014/26

**CT 105
COTER 118
COSI 135
COPS 511
JAI 1124
RELEX 1151
ENFOPOL 310
IXIM 184
HYBRID 101
CYBER 363
COMET 34**

NOTE

From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	EU counter-terrorism 25 years after 9/11: Evolving policies, lessons learned and the road ahead

Introduction

History has shown that terrorist acts can have a real strategic impact and an effect that transcends national borders. Terrorism and geopolitics are interlinked. The fight against terrorism is therefore – as it has been for the past two decades – an important aspect of EU security policy and external action. The events that took place in the United States on 11 September 2001, when 19 al-Qaeda members boarded four commercial aircraft and carried out the deadliest terrorist attack in history, reshaped the global security landscape and marked a fundamental shift in the way terrorism was understood and addressed internationally. In the years that followed, the evolving terrorist threat and counter-terrorism featured among the EU's security priorities, leading to new legislative frameworks and institutional structures and enhanced cooperation among EU Member States.

It is essential that the experience gained in counter-terrorism over the past two decades be properly assessed so that it can feed into ongoing and future discussions about the EU's response to terrorism. The present document therefore includes a brief historical perspective of the EU's response to terrorism, highlighting its development and the main lessons that have emerged along the way, but it does not seek to provide a comprehensive history of terrorism or counter-terrorism in Europe.

This document reflects the perspective of the Office of the EU Counter-Terrorism Coordinator (EU CTC), itself being a counter-terrorism instrument established in the wake of the Madrid terrorist attacks in 2004¹. The document also looks forward, reflecting on the possible evolution of the terrorist threat and its implications for the EU's internal security and external action, as well as the resulting policy challenges. It concludes with recommendations aiming to strengthen the EU's resilience and ensure that its counter-terrorism policy anticipates developments, addresses any vulnerabilities and remains ahead of the constantly evolving threat.

¹ European Council Declaration to Combat Terrorism of 25 March 2004, European Council Declaration to Combat Terrorism of 25 March 2004 and the European Council Stockholm Programme of 10-11 December 2010.

I. MAJOR ADVANCEMENTS IN EU COUNTER-TERRORISM SINCE 9/11

1. Al-Qaeda and the aftermath of 9/11: the urgent need to strengthen cooperation

9/11 and its aftermath exposed how EU territory was used by al-Qaeda for planning, recruitment and facilitation purposes before the terrorist attacks. It also confronted the EU with the realisation that its threat picture varied across Member States. In reaction to this, Member States agreed on a shared objective: to strengthen cooperation and enhance information sharing².

The establishment of Eurojust, which was already in its embryonic phase, was sped up and took place formally in February 2002³, with the aim of assisting Member States in particular in cross-border terrorism investigations⁴. In that same year, the first Council Framework Decision on Combating Terrorism⁵ provided a common legal basis for prosecuting terrorist offences. Prior to that, in 2001, the EU had focused its efforts on disrupting the operational capabilities of al-Qaeda in Europe by creating a sanctions regime to combat terrorism, borrowing elements from the sanctions mechanism already existing in the UN⁶.

2. Terror at the heart of Europe: the 2004 Madrid terrorist attacks trigger EU policies

The 2004 Madrid bombings brought the terrorist threat to the heart of Europe and triggered an immediate EU response focused on enhancing coordination at EU level. The European Council adopted a declaration on combating terrorism on 25 March 2004. It was an early example of the European Council taking the lead in shaping the response to major events and crises.

² It should be noted that, in the wake of the bombings of the Embassies of Kenya and Tanzania by al-Qaeda, in August 1988, a Council Decision was adopted on 3 December 1998 instructing Europol to deal with crimes committed or likely to be committed in the course of terrorist activities (Council Decision of 3 December 1998 instructing Europol to deal with crimes committed or likely to be committed in the course of terrorist activities against life, limb, personal freedom or property (OJ C 26, 30.1.1999, p. 22), repealed by Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol)).

³ Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust.

⁴ The European Council also requested the creation of a specialised unit within Europol, the CT Task Force. By this time, the first US-Europol (operational) cooperation agreements had been signed.

⁵ Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism.

⁶ Council Common Position 2001/931/CFSP on the application of specific measures to combat terrorism.

The Treaty on European Union stipulates in Article 4(2) that national security remains the sole responsibility of Member States. Up to 2004, the EU was not an actor in combating terrorism and preventing radicalisation: these areas were covered under the national legislation of the Member States⁷. Therefore, one of the first decisions the European Council took following the Madrid attacks was to establish the role of the EU CTC, who was tasked with presenting policy recommendations and proposing priority areas for action to the Council based on identified gaps and needs⁸. Subsequently, in 2005, the first EU Counter-Terrorism Strategy was issued, a fundamental document that guided policies over the years that followed⁹. The 2005 terrorist attacks in London reinforced the EU's collective will to counter terrorism in all its forms.

3. The rise of Islamic State and the threat posed by foreign terrorist fighters: urgent need for European action confirmed

In 2013, the Islamic State of Iraq (ISI), the successor of al-Qaeda in Iraq (AQI), expanded into Syria and was renamed the Islamic State of Iraq and al-Sham (ISIS, IS, or Da'esh). The so-called 'IS Caliphate' was proclaimed in 2014 and Europe was directly affected. IS developed a sophisticated and highly effective online propaganda machine exploiting the grievances resulting from and the impact caused by the Syrian civil war, and mobilised thousands of European citizens to join it – and to return to strike at the heart of Europe. The Paris attacks in November 2015, followed by the Brussels attacks in March 2016, marked a profound change in the nature and severity of the terrorist threat and pushed terrorism – once again – to the top of the EU's security agenda.

⁷ Nevertheless, terrorism had not been absent from the EU's agenda. The Trevi (Terrorisme, Radicalisme, Extremisme et Violence Internationale) group – an informal intergovernmental network – was established by the JHA Council in December 1975. The TWP was inaugurated in 1992 under the then 'third pillar', while COTER was set up in 1997.

⁸ The European Council's Declaration on Combating Terrorism of 25 March 2004 establishes the mandate of the EU CTC 'to co-ordinate the work of the Council in combating terrorism and, with due regard to the responsibilities of the Commission, maintain an overview of all the instruments at the Union's disposal with a view to regular reporting to the Council and effective follow-up of Council decisions'. The mandate was revised and expanded by the European Council on 10 and 11 December 2010, which confirmed 'the role of the EU Counter-Terrorism Coordinator in ensuring implementation and evaluation of the Counter-Terrorist strategy, coordinating Counter-Terrorist work within the Union, and fostering better communication between the Union and third countries'.

⁹ 14469/4/05 REV 4.

3.1. 2015–2018: closing the gaps

The aftermath of the devastating attacks in Europe was characterised by rapid operational adaptation to the novel threat. In January 2016, the European Counter Terrorism Centre (ECTC) was established within Europol as a central operational and information exchange hub. The EU's response followed three main lines: (i) countering online propaganda, with the creation of the EU Internet Forum¹⁰; (ii) preventing terrorist travel, by putting forward the EU Passenger Name Record Directive (PNR)¹¹; and (iii) hindering capabilities through the Firearms Directive¹², which implemented stricter controls on the acquisition and possession of weapons.

The landmark piece of EU legislation from that period is the Directive on Combating Terrorism¹³, adopted in 2017, which introduced minimum harmonisation on the definition of terrorist offences and offences relating to a terrorist group and terrorist activities across the EU. Specifically, it criminalises training and travelling for terrorist purposes. That legislation marked a shift from a primarily reactive approach to a more preventive EU-wide model of counter-terrorism. It provides all Member States with a harmonised criminal law framework to intervene at an earlier stage against any preparatory actions, including recruitment, terrorist training and the dissemination of terrorist propaganda.

¹⁰ Launched by the Commission in December 2015.

¹¹ 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.

¹² Directive (EU) 2017/853 of the European Parliament and of the Council of 17 May 2017 amending Council Directive 91/477/EEC on control of the acquisition and possession of weapons.

¹³ Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism.

The EU's counter-terrorism toolbox – that is, the set of legislative and non-legislative instruments developed in order to prevent and respond to terrorist threats – continued to evolve to reflect a changing threat landscape. Thus, the Schengen Information System (SIS) Upgrade (2018)¹⁴ strengthened the role of that system in counter-terrorism and law enforcement cooperation, including through the enhanced use of biometric data and improved information sharing.

3.2. 2019-2024: building resilience in the digital age

The territorial defeat of ISIS in March 2019 transformed it into a decentralised, widely dispersed and digitally-enabled terrorist organisation, capable of inspiring lone actors to perpetrate attacks of varying levels of sophistication without any direction. The online world thus became the new battlefield for counter-terrorism.

The EU's response increasingly focused on resilience, prevention and the security challenges posed by the online environment. To counter the scale and reach of terrorist propaganda across the EU, the EU's first legally binding instrument to mandate specific content moderation rules for online hosting service providers – the Terrorist Content Online (TCO) Regulation¹⁵ – was adopted in 2021. It established obligations for online platforms to remove terrorist content within one hour of a removal order being issued by the competent authority of a Member State. In 2022, the Digital Services Act (DSA)¹⁶ introduced a set of rules relating to illegal content, systemic risks and transparency.

¹⁴ Regulation (EU) 2018/1861 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 border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006. 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, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU. Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals.

¹⁵ Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

¹⁶ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

Expanding the focus on prevention, the Commission built on the Radicalisation Awareness Network, established in 2011, by launching the EU Knowledge Hub on Prevention of Radicalisation in 2024. It created a more robust EU-level platform for expertise and cooperation between policymakers, researchers and practitioners, enabling knowledge to be consolidated in order to drive evidence-based decision-making.

Although lone actor attacks of a low level of sophistication remained the main terrorist trend in the EU, there was a need to scale up measures in order to face up to the potential disruption from technologically enhanced terrorist capabilities. Issues relating to generative AI, for example, were addressed by the AI ACT¹⁷, adopted in 2024, to be implemented in a phased manner. That legislation marked the first step towards preparing the EU for a next generation of terrorism shaped by technological advancements.

4. 2025-2026: secured and modernised frontiers (biometric security)

The security of the EU and its citizens rests on Member States' ability to detect threat actors and assess their intentions, while exchanging information swiftly and efficiently. With that in mind, the EU's main databases became increasingly interoperable, creating an architecture to provide a safety net against external threats.

¹⁷ 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.

The introduction of the Entry/Exit System (EES)¹⁸ and the upcoming European Travel Information and Authorisation System (ETIAS) system¹⁹ – both in the making since 2017 – are the latest border security building blocks benefiting counter-terrorism across the EU. The EES ensures that all non-EU nationals provide their biometric data when entering the EU Schengen external borders²⁰, while ETIAS will change the way in which visa-free nationals travel into the Schengen area, by applying for travel authorisation online.

With the addition of those new instruments to the CT toolbox, the EU's external borders gain another layer of protection: among other objectives, the measures aim to help the authorities verify the identity of individuals, pinpoint any potential threats and prevent individuals linked to terrorist activities from exploiting gaps in border controls.

¹⁸ Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes.

¹⁹ Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226.

²⁰ Although the start of implementation has faced delays.

II. LESSONS LEARNED IN 25 YEARS OF EU COUNTER-TERRORISM POLICY

Over the past 25 years, the EU's counter-terrorism policy has evolved from a reactive framework into a broad and permanent security architecture. The evolving threat has repeatedly challenged existing policies and driven forward the implementation of new instruments that, collectively, constitute the EU's counter-terrorism toolbox. Informed by this long experience, at least 10 conclusions can be drawn today.

1. **Cooperation constitutes the backbone of the EU's counter-terrorism policy.** Member States' exclusive competence regarding national security remains the core principle underpinning any EU CT-related efforts. However, given the diverse, complex and cross-border nature of the terrorist threat, no Member State can effectively counter all those dimensions on its own. Counter-terrorism has thus evolved from a diverse range of national measures to an EU-level framework that respects the sovereignty of each Member State in security matters while leveraging the EU's collective weight and instruments. Although the terrorist threat has remained asymmetrical in nature across the EU over the past 25 years, counter-terrorism policymaking has fundamentally been a joint EU effort undertaken in the context of an unbreakable commitment of Member States' reciprocal assistance and support.
2. **Better cooperation requires a solid architectural foundation.** The central role played by the Justice and Home Affairs (JHA) Council, supported by the relevant Working Parties in the Council (in particular TWP²¹ and COTER²²), ensures that EU CT policies – in terms of both their internal and their external dimension – are grounded in Member States' expertise and intelligence; that EU efforts complement those of Member States; and that any gaps and needs are effectively addressed at EU level. In the past two decades, by adopting a Team Europe approach, the EU has built up an *acquis* that enhances Member States' CT capabilities through the horizontal reach of the EU CTC, the Commission's legislative and non-legislative initiatives, the intelligence shared by the Single Intelligence Analysis Capacity (SIAC), strong operational cooperation through EUROPOL, EUROJUST and FRONTEX and the contribution made by the EEAS, including through leading formal bilateral counter-terrorism dialogues with third countries and its wide network of counter-terrorism experts posted around the world.

²¹ Working Party on Terrorism.

²² Working Party on Terrorism – International Aspects.

3. **The continuous changes in the nature and urgency of the threat demand policy tools that are both flexible and adaptable.** EU counter-terrorism policy is a process of continuous adaptation to an unpredictable and evolving threat. The success of the decisions taken and of the policies adopted has had an impact on the EU's security as a whole: law enforcement and judicial cooperation structures, interoperable databases, sanctions regimes, border management tools and measures to counter terrorist financing contribute to the overall security of EU citizens. The EU is now better placed to tackle organised crime, trafficking in illicit goods and markets, hybrid threats and other forms of cross-border crime. Therefore, the EU's investment in counter-terrorism has generated both positive externalities and a significant return.
4. **The technological evolution continues to transform both the threat and the policy response.** The online ecosystems have become the global operational space for terrorism (and violent extremism), fundamentally changing the scale and speed of radicalisation, recruitment and mobilisation – regardless of affiliation. Addressing that online dimension remains an ongoing and urgent priority.
5. **The pace of implementation of EU counter-terrorism policy does not always keep up with the evolution of the threat.** EU legislation and its implementation across the EU necessarily take time, and might therefore be lagging behind the pace at which the terrorist threat evolves. This time lag becomes even more pressing as new technologies enhance the terrorist threat both now and in the future. Nevertheless, the ability to maintain a comprehensive and continuous overview of gaps and needs, including through the role of the EU CTC, has been critical in terms of ensuring an appropriate degree of anticipation.
6. **The EU's counter-terrorism strategy has progressively shifted from reaction to prevention.** One of the main lessons learned is that long-term success is not only about disrupting attacks, but also about building resilience through a whole-of-society approach, involving communities, civil society, the private sector, institutions and other relevant actors in preventing radicalisation, countering extremist narratives and reducing the wider impact of terrorism.

7. **The EU's internal and external security are fundamentally interconnected.** Geopolitical developments and crises outside the EU's borders have a direct impact on the EU's internal security. The approach adopted by Member States in the JHA domain over the past two decades in continuously advocating²³ for the importance of connecting the internal and external EU policy domains has borne fruit. It has ensured that EU policies reflect Member States' counter-terrorism concerns and complement efforts undertaken at national level.
8. **Effective counter-terrorism requires international cooperation.** The EU, through the instruments at its disposal, including a network of delegations and formal counter-terrorism dialogues, has provided an opportunity for cooperation and exchange of information with third countries and partners that individual Member States may not have contact with. Furthermore, the EU has maintained its leadership in international fora and multilateral institutions, such as the UN, the Global Coalition against Daesh and the Global Counterterrorism Forum, and has also played a fundamental role in providing support to partners in counter-terrorism capacity building and prevention of violent extremism.
9. **The EU counter-terrorism policy must be informed by the intelligence of EU Member States.** The SIAC has been of paramount importance in terms of providing the required threat assessments and foresight analyses that have underpinned the EU's policies. Considering the politicisation of counter-terrorism policies in some parts of the world, it is especially important to maintain objective assessments of the nature of the terrorist threat in the EU and beyond.
10. **The EU counter-terrorism policy requires communication in the public domain.** This is essential in order to avoid any misperceptions and explain how compatibility with fundamental rights and the rule of law is ensured. Legitimate and important discussions about proportionality, privacy and freedom of expression must be informed by practitioners in the field of law enforcement and counter-terrorism in order to preserve the appropriate balance between the various fundamental rights.

²³ As reflected in the EU CTC's mandate since 2004.

III. FROM THE POST-9/11 PARADIGM TO THE FUTURE THREAT ENVIRONMENT: KEY SHIFTS AND DRIVERS

The shape, scope and severity of the terrorist threat have changed significantly since 9/11. While existing terrorist organisations remain a security priority, they now exist among a broader and more diffuse threat landscape. Easier access to capabilities, changing patterns of radicalisation, interaction with other security threats and the vertiginous pace of technological developments all have an influence in terms of who poses a threat, how attacks are prepared and what potential impact such attacks may have.

1. **Widespread access to capabilities that can be used for terrorist purposes.** Terrorist activity is no longer the exclusive realm of structured organisations that provide ideological indoctrination, leadership, training, financing and operational support. Instead, lone actors or small groups can easily obtain access to knowledge, expertise and tools without any centralised direction or affiliation.
2. **Spread of the terrorist threat across a wider spectrum, ranging from ideological mobilisation to stochastic violence²⁴.** Although ideological commitment and political change remain the key defining features of terrorism and violent extremism, violent mobilisation is likely to be increasingly shaped by a wider combination of factors, including individual grievances, personal vulnerabilities, social polarisation, single-issue causes or any random form of opportunistic motivation.
3. **Technology as the key strategic enabler and accelerator of the terrorist threat.** Technological developments will continue to accelerate many of the shifts shaping the terrorist threat, and the pace of change is likely to become increasingly difficult to keep up with. However, history has proven that terrorist actors adapt quickly, exploiting technological innovations to enhance their reach, their capabilities and their disruptive impact. The key issue here is therefore not simply the technological innovations themselves, but rather the gap between the speed of terrorist actors and that of the security institutions in using those innovations for their own respective ends.

²⁴ For example, nihilistic extremist violence.

4. **Changing patterns of radicalisation and recruitment.** Digital platforms will continue to transform the scale and speed at which the various actors can reach out to and influence individuals. Minors and young adults – ‘digital natives’ – are especially vulnerable, as their online and offline lives increasingly merge together into the *onlife* experience²⁵. As AI-generated content and personalised interactions evolve, they will enable further tailored messaging and conversations adapted to individual users, thereby further transforming the radicalisation processes and creating added challenges in terms of detection and prevention.
5. **Terrorism-as-a-service and the wider use of terrorist tactics.** The volume of terrorist operational knowledge which is available online and readily accessible attracts individuals, as terrorism tactics are no longer the exclusive remit of terrorist actors. In fact, financial gain can also replace ideology and serve as a mobilising factor. Seeking the same impact as that achieved by terrorism – instilling fear, undermining democratic rule, polarising communities and influencing political outcomes – terrorist tactics may increasingly be used as part of a wider disruptive toolkit by hostile state actors. While their motivations and goals remain distinct, the overlap in methods complicates prevention, attribution and response.
6. **A growing overlap of threats while maintaining distinct identities.** There is an increasing level of interaction between terrorism and violent extremism, organised crime and hostile state activities. Those elements encompass distinct drivers, objectives and strategic gains. However, the overlap between them contributes to a more severe threat. The security landscape increasingly resembles a Venn diagram, where different threats retain their identity, but share overlapping spaces in terms of tactics, capabilities and networks. This overlap allows for methods from different domains to be borrowed and adapted, creating a more complex and fluid security landscape, where threats no longer remain confined within specific borders.

²⁵ Term coined by the Italian philosopher Luciano Floridi, chair of the EU’s Onlife initiative (2012-2013).

7. **Geopolitical conflicts providing fertile ground for terrorism to take root, consolidate and expand.** Over the past 25 years, terrorism has thrived in the fertile ground created by conflict and instability. The consequences of past and ongoing conflicts will continue to linger and shape the terrorist threat affecting the EU's internal security. External security will therefore continue to constitute a key dimension of the EU's counter-terrorism policy, and sustained cooperation with international and regional partners will remain essential in order to address the threats before they reach Europe.

IV. **THE WAY FORWARD: SHAPING EU COUNTER-TERRORISM POLICY FOR THE NEXT 25 YEARS**

The EU and Member States have developed a substantial and robust counter-terrorism framework over the past two decades. Many stakeholders deserve credit for that achievement, and even more will need to be involved in the future in order to continue to develop and adapt effective CT strategies as the terrorist threat landscape continues to evolve. Collective efforts will require a shared awareness of the nature of the terrorist threat and a continued commitment to deploying all the appropriate EU instruments to counter it.

The following eight recommendations may guide policymakers as they shape counter-terrorism efforts at EU level in the years to come.

- i. **Maintain a common understanding of the evolving terrorist and violent extremist threat within the security landscape.** The evolution of the threat and its more fluid nature raise difficult questions as regards what falls within the scope of counter-terrorism and what should be addressed through other frameworks. While this does not mean that the existing definitions need to be revised, updated or widened, it is essential to ensure that any new decision-making continues to be aligned with the evolving threat, and that any grey areas or empty spaces are decisively addressed.

ii. **Build on existing institutional structures and mandates rather than create new ones.**

Over the past 25 years, the EU has developed a solid body of expertise across its institutions. Importantly, existing structures and mandates have allowed the EU to maximise its role in complementing Member States and respecting their primary competence in the internal security domain as well as Member States' exclusive responsibility over national security. As new challenges and threats emerge – currently in the hybrid domain, but of an unknown nature in the future – this approach should be continued while adjusting any existing structures as necessary.

iii. **Pool resources and strengthen Member States' capabilities** to ensure that the counter-terrorism protective net remains tightly secured across the EU. The technology-enhanced future threat will require expertise, capabilities and resources (both human and financial) that will exceed what Member States are able to muster on an individual basis. Burden-sharing, pooling of resources and the development of joint capabilities will add value and give the EU a strategic advantage when countering the threat.

iv. **Anticipate and prepare for emerging and disruptive technologies.** Technological change needs to be a continuous overarching security strategic priority, bearing in mind that its impact goes far beyond terrorism. Artificial superintelligence and advanced autonomous systems are already having an impact on our security environment. Future developments will affect the capabilities of both state and non-state actors and will potentially create new gaps in terms of the protection of our citizens. Anticipation, preparedness and resilience require scientific and technical expertise (including through the Commission's Joint Research Centre), as well as closer links with industry. Sustained and systematic investment is needed in order to create the joint capabilities that will allow us to exploit important new technologies for the benefit of law enforcement and counter-terrorism.

v. **Invest in research and innovation for a more effective counter-terrorism policy.**

Research improves the understanding of emerging threats and evaluates existing measures. Innovation supports the development and testing of new tools and instruments to address evolving challenges. Bringing research and innovation together will help turn knowledge into practical solutions and ensure that future counter-terrorism policies are targeted, effective and fit to respond to the evolving threat landscape.

- vi. **Ensure that legislative initiatives keep pace with the digital environment and new technologies.** The critical battle against terrorism and violent extremism will in large part be fought online. It is therefore of paramount importance that law enforcement and intelligence should be sufficiently well equipped to address the online and digital threat. Legitimate concerns regarding the protection of fundamental rights, including privacy, must be balanced against legitimate security considerations. In fact, those concerns can and should be addressed, not by delaying the adoption of urgent tools, but by reinforcing safeguards as regards the proportionality and effectiveness of their use.
- vii. **Strengthen societal resilience.** Prevention remains the essential long-term strategy for countering terrorism and violent extremism. The EU has moved from a *whole-of-government* approach brought about by 9/11 to a *whole-of-society* approach adopted as the core pillar for preventing and countering violent extremism 10 years ago. The future will require an even more integrated approach. A *whole-of-systems*²⁶ strategy is needed – one that encapsulates the many different dimensions that determine the future terrorist threat: the online environment; and the wider security, societal, technological, public and private sector, criminal, financial and geopolitical environments.
- viii. **Preserve specialised expertise while ensuring synergies.** Although there are overlaps in terms of the tactics and actors involved, the threats from terrorism, violent extremism, organised crime and malign states are distinct and must not be conflated with one another. The EU's response in countering them requires the appropriate combination of existing types of expertise, dedicated frameworks and toolboxes and fundamentally different strategies. However, this does not mean that strategies adopted in one domain should not benefit from insights in other domains. Identifying and recognising some of the overlaps between different threats – for instance, in the counter-terrorism and hybrid domains – can benefit EU policymaking and coordination between Member States. This requires regular consultations between the JHA, foreign affairs, telecommunications and other policymaking communities in order to establish a comprehensive threat picture and identify areas for enhanced synergies. This will ensure that no gaps in our collective security remain unaddressed simply because they fall outside the remit of one traditional domain or mandate or because they cannot easily be categorised.

²⁶ A term introduced by researchers in the last couple of years.