Council of the European Union

Brussels, 12 December 2024
(OR. en)

16820/24

CT 128
ENFOPOL 523
COTER 250
JAI 1859

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	12 December 2024
To:	Delegations
No. prev. doc.:	16020/24
Subject:	Council conclusions on future priorities for strengthening the joint counterterrorism efforts of the European Union and its Member States – Council conclusions (12 December 2024)

Delegations will find in the annex the Council conclusions future priorities for strengthening the joint counterterrorism efforts of the European Union and its Member States, approved by the Council (Justice and Home Affairs) at its 4068th meeting held on 12 December 2024.

———————————

Council conclusions

on

future priorities for strengthening the joint counterterrorism efforts of the European Union and its Member States

Introduction

a) Terrorism and violent extremism, as well as radicalisation, continue to pose a significant threat to the European Union and its Member States, and therefore counterterrorism and preventive efforts should remain a high priority.

b) Destabilising internal and external events, such as Russia's war of aggression against Ukraine and the ongoing conflict in the Middle East, have heightened the terrorism threat level in some Member States and contributed to the intensification of radicalisation and social polarisation, potentially leading to terrorism and violent extremism across the Union.

c) The terrorism threat is more complex than ever and is driven by various factors. These include the risk posed by lone actors, the increased external threat projection of Islamic State, including its Khorasan Province (ISKP) branch, the misuse of new technologies by terrorist groups and actors, the growth of violent anti-system extremist movements not attributed to specific ideologies and the blurring of ideologies leading to a mix of violence-prone beliefs. Jihadist terrorism remains the most prominent threat to the European Union, while the threat from violent right-wing extremism remains high in some Member States.

d) Radicalisation remains a key concern, in which the online space plays an important role, particularly among minors, allowing the rapid spread of terrorist content and fuelling social polarisation which may be exacerbated by foreign information manipulation and interference (FIMI), including disinformation activities by state and non-state actors.

e)   We must continue preventive efforts aimed at supporting local actors and practitioners, enhancing community resilience to radicalisation, and increasing collaboration with educational institutions, communities, and faith groups. It remains important to counter radicalisation in prisons, especially addressing the risks related to the release of radicalised inmates and those sentenced for terrorist offences. Additionally, it is crucial to ensure that national and European funds do not inadvertently support individuals and organisations pursuing an illegal agenda or promoting values incompatible with those enshrined in Article 2 TEU of the European Union.

f)   Concerns remain that suspected third-country foreign terrorist fighters and individuals linked to terrorist groups may exploit migratory flows to infiltrate the European Union. Great efforts have been made to strengthen detection, improve information exchange and external border controls. However, Member States must continue their efforts to detect and prevent the entry and movement of such individuals within the EU's territory.

g)   At the same time, the return of third-country nationals who pose a security threat and are staying illegally in the EU remains a significant challenge and their continued presence within the EU presents an ongoing security risk. It is therefore crucial to ensure the efficient and swift return of people who do not, or no longer, have a right to stay and who represent a security threat. In addition, we need to continue exploring solutions to address the security threat posed by individuals who cannot be returned to their country of origin due to the principle of non-refoulement, in full accordance with applicable EU law and international law.

h)   Good progress has been achieved over the past five years in the field of countering terrorism and violent extremism, and preventing radicalisation, the Commission's EU Counter-Terrorism Agenda has been effectively implemented. Progress has also been made in other relevant internal security policies and initiatives that facilitate the work of counterterrorism authorities, such as improved information exchange.

i)   Council Conclusions adopted in recent years[1] remain highly relevant and should be fully implemented. Together with the six-monthly EU threat assessments in the field of counterterrorism, they continue to provide a comprehensive framework for action.

General considerations:

1.   Member States remain committed to countering terrorism and violent extremism in all its forms and manifestations to ensure the security and safety of their citizens, while upholding the values of democracy, fundamental rights, and the rule of law. Member States, the Commission and EU agencies have all been working diligently to strengthen the Union's resilience against terrorism and violent extremism and should continue to work on collective actions and enhance their cooperation.

2.   Parallel to this set of conclusions, the Council will adopt Conclusions on reinforcing external-internal connections in the fight against terrorism and violent extremism. In this context it is recalled that in December 2020 the European Council reaffirmed the role of the EU Counterterrorism Coordinator (EU CTC). The EU CTC has a key role in coordinating counterterrorism work within the Union, in reinforcing the Union's CT relations with third countries and in enhancing the links between internal and external aspects of CT-efforts. The EU CTC is also tasked to follow up the implementation of Council Conclusions on the fight against terrorism.

3.   To effectively respond to the evolving threat landscape, and in the light of the new institutional cycle and the review of the EU's strategic framework on internal security, there is a need to adapt and further strengthen the European Union's counterterrorism strategy together with the Member States. The Council therefore welcomes the fact that the political guidelines for the new Commission's mandate highlight the need for a new EU Agenda for Preventing and Countering Terrorism and Violent Extremism to address new and emerging threats.

---

[1]   9997/22; 16335/23; 16336/23.

4.   In this set of Conclusions, the Council highlights key areas where increased efforts are needed to enhance operational efficiency and sets strategic goals. The aim is to shape EU counterterrorism policies and measures, including in the area of prevention, for the next five years.

I.   **Horizontal policy requirements contributing to a high level of internal security and the effectiveness of counterterrorism measures**

5.   While respecting the fact that national security remains the sole responsibility of each Member State, a comprehensive and coordinated European approach transcending individual policy areas and integrating overarching principles is needed to effectively combat terrorism and violent extremism. Further synergies between the Terrorism Working Party (TWP) and other Council preparatory bodies, particularly the Working Party on Terrorism (International Aspects, COTER) and the Working Party on restrictive measures to combat terrorism (COMET), should be explored to address the terrorism threat in a holistic manner, while respecting the mandate and specific focus of TWP.

6.   We need a balanced approach that safeguards all fundamental rights, including the right of European citizens to both security and privacy. To this end, we need to amplify the voice of the counterterrorism and internal security community entrusted with protecting our society by promoting a positive narrative that underscores their legitimate operational needs.

7.   Lawful access to and retention of data, including legally and technically sound solutions to access electronic communication in readable format, is essential for the successful detection, prevention, investigation, and prosecution of terrorist activities. Therefore, law enforcement and counterterrorism authorities must have the ability to access digital data effectively in full respect of fundamental rights and the relevant data protection laws, while upholding the principles of necessity, proportionality and subsidiarity and without generally weakening encryption which is recognised as an important means for protecting the cybersecurity of governments, industry and society.

8.	It is vital that communication service providers fully comply with the legal requests related to lawful access to data by law enforcement and counterterrorism authorities in accordance with the applicable legal obligations. Furthermore, it is essential that technology providers and communication service providers engage with authorities when they develop and apply new technologies and services.

9.	Counterterrorism and judicial authorities should be supported in their efforts to combat terrorism and violent extremism, including through training, capacity building, and the provision of appropriate resources. The flexible allocation and effective use of EU funding can significantly enhance these efforts without the current set of conclusions prejudicing the future multiannual financial framework.

10.	Investment in security research and innovation that supports counterterrorism efforts, including fostering innovative solutions in border management, AI tools, big data analytics, decryption technologies, biometric data analyses and digital forensic tools, is key for law enforcement and counterterrorism authorities to keep up with rapidly evolving technologies.

11.	Assessment and briefings by the EU Intelligence and Situation Centre (INTCEN), based on strategic intelligence from Member States as well as the analyses of Europol, should be taken into account when formulating counterterrorism policies and measures to effectively address the evolving threat landscape. In order to foster intelligence-based situational awareness, it remains important to strengthen the EU Single Intelligence Analysis Capacity by enhancing its resources and capacities in line with the objectives of the Strategic Compass.

12. Terrorism financing poses a critical and systemic threat to security by enabling groups to recruit, plan, train for and carry out attacks. Funds collected in Europe are not only directly used in Europe but also sent to terrorist organisations abroad helping them to build capacity to carry out attacks on European soil. Digital technologies, such as virtual assets and online platforms, are increasingly exploited for this purpose, whereas traditional financing methods, such as cash payments and hawala, remain widely used and difficult to trace. Furthermore, terrorist organisations increasingly exploit external conflicts to raise funds also in the EU, masking their violent intentions under the guise of charitable activities. Therefore, Member States' capacity to successfully identify, trace, investigate and prosecute the financing of terrorism as well as to freeze and seize such funds and assets must be strengthened and supported. It is also important to enhance private-public partnerships with relevant stakeholders to foster better access to financial information.

13. At the same time, joint efforts are needed to limit the financial means of groups and actors, including all forms of violent extremist groups, promoting radicalisation, hatred or values contrary to those enshrined in Article 2 TEU. This encompasses actions against undesirable foreign funding. The ongoing work in the EU Internet Forum and global public-private counterterrorism initiatives are also important in order to counter the online financing of such groups and actors.

14. Efforts to prevent terrorists and violent extremists from accessing firearms, explosives, and CBRN (chemical, biological, radiological, and nuclear) materials, and efforts to counter the malicious use of drones, must continue. This includes closing potential remaining gaps in the regulatory framework and its implementation; improving the detection capacity of Member States; and addressing challenges posed by emerging technologies, such as 3D-printing. Continued cooperation with Ukraine and the Western Balkans is vital to curbing firearms trafficking into the Union.

In this context, the COUNCIL invites the MEMBER STATES to:

15. enhance their preparedness and response capabilities in relation to potential terrorist and violent extremist attacks. This can be done through regular exercises, close cooperation, and the sharing of best practices, as well as by increasing the involvement of counterterrorism authorities in the European Multidisciplinary Platform Against Criminal Threats (EMPACT), as appropriate;

16. continue allocating appropriate resources for research and innovation in the field of counterterrorism and law enforcement and provide expertise for the EU Innovation Hub for Internal Security.

and invites the COMMISSION to:

17. ensure the necessary support for internal security agencies and networks, particularly Europol's European Counter Terrorism Centre (ECTC), Europol´s Analysis Project Weapons and Explosives, the EU Innovation Hub and the ATLAS network. The aim is to enable these to scale up and tailor their assistance and operational support to meet the specific needs of Member States;

18. allocate the appropriate research funding to internal security-related projects, with a particular focus on addressing the specific needs of counterterrorism authorities and supporting the uptake and deployment of innovative solutions;

19. enhance its dialogue with the online platforms and develop an effective approach for the implementation of the recommendations of the High-level Group on Access to Data for Effective Law Enforcement which address the law enforcement authorities' needs to access electronic communications in order for them to carry out their tasks effectively and lawfully and, in full respect of fundamental rights, to prevent, detect and investigate criminal offences;

20. develop a comprehensive strategy to prevent and counter terrorism and violent extremism by taking into account the key intervention areas and suggested measures listed in these Conclusions, as well as by taking forward the initiatives put forward by recent Council Conclusions. This work needs to be done in collaboration with the Member States and through the new internal security strategy and the EU Agenda for Preventing and Countering Terrorism and Violent Extremism.

and invites the COMMISSION and the MEMBER STATES to:

21. reflect on the way forward in relation to frameworks for administrative measures on capital movements and payments such as the freezing of funds, financial assets or economic gains to limit financing of terrorism and violent extremism in all its forms, consistent with the objectives set out in paragraphs 12 and 13.

II. **Key intervention areas for strengthening counterterrorism efforts**

    i) <u>Information exchange</u>

22. It is essential to enhance and improve the entering of information into European databases, using to the fullest extent particularly the Schengen Information System (SIS), but also the Europol Information System (EIS) and the Europol Analysis Projects, and Interpol databases, in line with the applicable EU and national law. These tools are essential in supporting Member States to detect and monitor individuals who pose a terrorist threat and should be continuously optimised.

23. Counterterrorism authorities need to have the necessary capacity to fully utilise information exchange tools, databases, and their interoperability. Accordingly, it is crucial to support these authorities in building the necessary capabilities, knowledge, and best practices to ensure the efficient and effective use of these resources in their operational work.

24. The work done to promote a shared understanding among the law enforcement authorities of the EU Member States, based on non-binding criteria, of which persons are assessed by the individual Member States to pose a terrorist or violent extremist threat, with a view to include this information in the European databases, is a step forward, without affecting the different national legislations in this regard.

25. It is important to make full use of Europol's mandate by finalising and concluding new international agreements that facilitate the exchange of personal data between Europol and priority third parties. In the absence of such agreements, in situations of imminent danger and on a case-by-case basis, with full respect of the applicable EU law, it remains vital to enable the swift exchange of personal data.

26. With a view to examining the options of making use of the data of travellers using maritime and land transport for law enforcement purposes, the Council looks forward to the Commission's presentation of its feasibility study on harmonising reporting obligations.

In this context, the COUNCIL invites the MEMBER STATES to:

27. enter all available data on individuals posing a terrorist threat into the relevant European databases and information systems and make full use of the possibility of entering terrorism-related alerts into SIS, in line with EU and national law and unless legal or operational considerations dictate otherwise.

invites the COMMISSION to:

28. present the way forward, following the upcoming evaluation of SIS and with due regard to feasibility and proportionality, on introducing a post-hit procedure for foreign terrorist fighters registered in SIS, based on the voluntary reception of hit notifications, in order to improve the information exchange.

and invites the COMMISSION and the MEMBER STATES to:

29. taking into account the findings of the upcoming feasibility study, and the jurisprudence of the European Court of Justice, further reflect on how the collection of data from travellers on land and maritime transport could be best used and integrated into information exchange practices.

and invites the COMMISSION to:

30. in light of the judgement of the Court of Justice of 21 June 2022 in case (C 817/19), evaluate the implementation of Directive 2016/681 ("the PNR Directive").

ii) <u>Detecting and preventing the infiltration of persons posing a terrorist threat</u>

31. There is a need to ensure robust border control and security, including systematic checks of all travellers against relevant databases at the external borders of the European Union, leveraging biometric data and other available technologies to prevent the undetected entry of individuals posing a terrorist threat on EU territory. These efforts will enhance the overall security of the Union.

32. To that end, the overall capacity of counterterrorism, border management, and immigration and asylum authorities needs strengthening, together with coordinated efforts to detect and prevent the infiltration of third-country individuals with connections to terrorist organisations at the earliest stages of entry into the Union.

33. The use of entry bans against third-country nationals representing a terrorist threat and the entering of data on these individuals in SIS, is a crucial tool to prevent foreign terrorist fighters entering into Europe. However, national legal and institutional frameworks between Member States on the issuance of entry bans vary. Accordingly, this can pose a challenge in terms of the issuance and recording in SIS of entry bans on individuals where there is no direct link or relation between those individuals and the issuing Member State. This should be addressed particularly by following up on the Council Conclusions 9997/22 adopted on 9 June 2022.

34. Where it is not possible to enter alerts for refusal of entry and stay in the SIS, the possibility to enter alerts for discreet, inquiry or specific checks, under Article 36 of the SIS Regulation (2018/1862) should be considered according to the specificities of each case. The information alert to be entered in the interest of the Union, once implemented, will be an additional instrument to cover cases where a third-country national poses a threat to the EU, but not necessarily to a specific Member State.

35. It is also important to step up efforts to identify the travel patterns and connections of individuals involved in terrorism or terrorism-related activities.

36. With due regard to fundamental individual rights, progress made in fostering cooperation between immigration and asylum authorities and counterterrorism authorities, particularly through the establishment of and voluntary participation in a network of points of contact, will facilitate cooperation and information exchange. The implementation of the Entry/Exit system (EES), the European Travel Information and Authorisation System (ETIAS) and the interoperability of European databases are important in this context.

37. It is crucial to enhance cooperation with transit countries and countries of origin to facilitate the exchange of information about persons posing a terrorist risk, as well as the efficient return of such individuals. In this regard, cooperation on the external dimension of migration and the use of all available instruments to intensify and strengthen relations with third countries in particularly through mutually beneficial partnerships are of key importance.

38. It is important to use the results of the EMPACT priority on High-Risk Criminal Networks (HCRN), Europol's HRCN mapping exercise on the most threatening criminal networks and the strategic intelligence provided by INTCEN to enhance understanding of the possible link between organised crime groups and terrorist organisations and to disrupt potential criminal connections.

In this context, the COUNCIL invites MEMBER STATES to:

39. continue to insert alerts based on return decisions in SIS; ensure appropriate use of the SIS alert on the return decision on a third-country national - indicating whether the person poses a threat to public policy, to public security or to national security. Member States are also asked to further align the use of such 'security flags' (in the meaning of Article 4(1)(o) of the SIS Regulation 2018/1860) throughout the return procedure by sharing good practices.

40. continue to issue national entry bans to third country nationals posing a terrorist threat, in accordance with their national law, and extend these measures to the Schengen area under Article 24 of the SIS Regulation 2018/1861. It is recalled that it is always considered proportionate to enter alerts in the SIS in cases related to terrorist offences, in particular if there are serious grounds for believing that a third-country national has committed a terrorist offence, or there are clear indications of intention to commit such an offence in the territory of a Member State.

and invites MEMBER STATES and the COMMISSION to:

41. continue to reflect on a way forward to facilitate the issuance of entry bans against third country nationals posing a terrorist threat, including in cases where there is no direct link or relation between those individuals and the issuing Member State.

42. work towards operationalising the effective return of persons posing a security threat by examining the possibility of optimising the legal framework to allow for an expedited return process for third-country nationals illegally staying in Member States' territories, especially when they are identified as security threats, as well as to jointly work towards strengthening the relationship with prioritised third countries and countries of origin to facilitate the expulsion of such individuals;

iii) Countering terrorism and violent extremism online

43. The digital sphere has increasingly become a breeding ground for radicalisation as terrorist and violent extremist organisations exploit online platforms to spread their ideologies, recruit followers, collect or transfer funds and incite violence, including through the use of information manipulation, with their messaging targeting and reaching an ever-younger audience.

44. Countering online terrorism and violent extremism, as well as radicalisation requires a coordinated and multifaceted approach that involves close cooperation between governments, online service providers, civil society, and law enforcement and counterterrorism authorities. The active involvement of Member States is key to strengthen this work.

45. Cooperation with online service providers should be intensified to address the proliferation of terrorist and violent extremist content and to encourage them to mitigate the spread and the algorithmic amplification of harmful but legal content fuelling social polarisation or misinformation that may lead to terrorism and violent extremism. The work within the EU Internet Forum is valuable and needs to continue to engage online platforms in preventing and countering the spread of such content.

46. With the adoption of the Regulation on addressing the dissemination of terrorist content online (TCO Regulation) and the Digital Services Act (DSA), significant progress has been made in holding digital service providers accountable for illegal content on their platforms. These Regulations should be fully implemented without delay and strictly enforced. There is also an urgent need to address the challenges posed by non-cooperating digital service providers.

47. Europol's dedicated online platform (PERCI) supporting the issuance and transmission of removal orders and referrals is an important step towards the efficient implementation thereof. Europol has also contributed significantly, particularly through the work of its Internet Referral Unit (IRU) and the organisation of referral action days aimed at tackling online terrorist content. Europol should continue these efforts.

48.   It is important that Member States are actively involved in shaping the activities of the recently launched EU Knowledge Hub on Prevention of Radicalisation. This will help ensure that its work programme aligns with the needs of Member States, policymakers and practitioners, and that its output is widely accessible and impactful among both policymakers and practitioners.

In this context, the COUNCIL invites MEMBER STATES to:

49.   continue efforts to enhance the shared understanding of terrorist propaganda activities and their impact on radicalisation and social polarisation leading to terrorism and violent extremism, with a particular focus on the impact of such propaganda activities on minors and the role of mental health in the process of radicalisation. The support of the Commission and relevant agencies as well as the collaboration with online service providers, civil society, and other stakeholders, as appropriate, are important in the context of this work.

and invites the COMMISSION to:

50.   continue to promote the sharing of best practices relating to the application of the TCO-Regulation, as well as to examine and address potential gaps in the regulatory framework and how to best align the implementation of the TCO Regulation and the DSA when evaluating the TCO-Regulation, while taking into account operational needs of law enforcement and counterterrorism authorities.

51.   take steps to address the challenges posed by non-complying online platforms by strictly enforcing the DSA in the case of very large online platforms and by continuing to cooperate with platforms and place adequate political importance on such cooperation, including in the context of the EU Internet Forum.

———————————