Council of the European Union

Brussels, 3 June 2024
(OR. en)

10406/24

LIMITE

CT 63
ENFOPOL 264
COTER 112
JAI 892

PUBLIC

NOTE

From:	Presidency
To:	Permanent Representatives Committee/Council
Subject:	Counterterrorism: Current challenges and Presidency initiatives and activities in the area

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (25.10.2024)

BACKGROUND

This paper sums up the Presidency focus areas and initiatives for the past six months in the domain of counter-terrorism (CT).

It is **important to be aware of challenges and set clear priorities for the EU's CT policy**, bearing in mind the changing threat landscape and that it will soon be time to start reflecting on the way forward with a new Commission and Parliament.

Maintaining a situational overview is a precondition for putting in place adequate countermeasures and requires Member States to systematically report incidents related to violent extremism and terrorism in all their forms, as well as continuous mapping of the EU measures in place.

CURRENT CHALLENGES AND INITIATIVES/MEASURES TAKEN

The threat landscapes across Europe vary depending on the nature and level of the main terrorist threat in each geographical area. However, jihadist terrorism remains the most prominent threat to the European Union (EU)[1]. **Islamic State Khorasan Province (ISKP)**, the Da'esh branch active in Afghanistan that is deemed likely to have been responsible for the recent attack in Moscow on 22 March 2024, **is assessed to pose an increased threat to Europe, where it is attempting to extend its scope of action**, and its capabilities and potential operational activities should be carefully monitored by relevant stakeholders **DELETED**. A number of Europe-based ISKP-affiliates/sympathisers, most of whom came from Central Asia and the North Caucasus, were arrested in Europe in 2023 on suspicion of supporting IS and of forming a terrorist organisation. **Continuing incidents involving the desecration of the Koran have exacerbated tensions, and international Islamist terrorist organisations**, including Da'esh, and individual supporters have called for revenge attacks. In the weeks following Hamas' attack on 7 October 2023 and the subsequent military response by Israel, France and Belgium witnessed terrorist attacks and there was a surge in antisemitic and anti-Muslim incidents, which led to **a number of Member States raising their national threat levels**. The Presidency, in the Working Party on Terrorism (TWP), has taken steps to ensure that a **comprehensive overview of the national threat levels** of the Member States and of changes thereto is available at any time.

[1] 9487/24: EU threat assessment in the field of counterterrorism.

Member States report incidents arising from **foreign information manipulation and interference (FIMI)** **DELETED** by foreign state and non-state actors[2]. Some Member States have been targeted by coordinated, staged campaigns of foreign origin attempting to mobilise and radicalise diaspora groups and groups with a low level of trust in authorities. In some cases, disinformation campaigns have started at national level, been picked up internationally and turned into FIMI activities. **In recent months, the Presidency has placed strong emphasis on the issue of FIMI, including in a CT context.** It is important to improve knowledge and understanding of this problem and its impact on violent radicalisation and terrorism. Dealing with FIMI requires synergistic actions to be taken, with due respect for the division of competences between the Member States and the EU. **The focus should be on early detection and countermeasures in the form of strategic communication and counter-narratives**. This demonstrates the importance of a continued and strengthened dialogue with internet providers/technology companies and with civil society and religious leaders.

PUBLIC

[2] EEAS definition of FIMI: 'Foreign information manipulation and interference in the information domain (FIMI), including disinformation, describes a mostly non-illegal pattern of behaviour in the information domain that threatens or has the potential to negatively impact universal values and integrity of government procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, often in relation to other hybrid activities. Actors of such type can be state or non-state actors, including their proxies inside and outside of their own territory.'

The risks associated with radicalisation leading to violent extremism and terrorism in **prisons**, and with the release of individuals who have either been convicted of terrorism-related offences or convicted of other criminal offences but become radicalised in prison and based on an individual risk assessment, are deemed to still pose a threat, need to be addressed by effective measures. Both prison and post-release reintegration efforts, and the adoption of probation measures, should be intensified when a given case is analysed and the individual in question found to pose a post-release risk. **Risk assessments of inmates during the detention period and, if necessary, following their release are important DELETED**. Social reintegration efforts made within prisons and after a person's release need to be strengthened. It is crucial to ensure continuity between the rehabilitation and reintegration efforts made within prisons and after release, and to encourage effective sharing between Member States' authorities of relevant information concerning the imminent release of prisoners convicted of terrorism or of radicalised inmates convicted of other criminal offences. It is crucial that **the exchange of information, through established information sharing mechanisms, between Member States on individuals posing a terrorist threat** and on risk assessment tools be further strengthened.

It is important that Member States and practitioners continue to be supported in reinforcing their capacities to prevent and counter violent extremism by the **EU Knowledge Hub on prevention of radicalisation**, which will be launched by the Commission in June, building on the achievements of the Radicalisation Awareness Network (RAN).

PUBLIC

Member States should continue their efforts to **recognise and handle, at an early stage, public security threats stemming from individuals considered by national law enforcement authorities to constitute a violent extremist/terrorist threat, and to include this information in European databases and information systems**, where possible and in line with national and EU legislation[3]. The need to further strengthen the sharing of information, within the existing national and EU regulatory frameworks, about such individuals when they travel or connect with individuals or networks in other Member States should be considered, while respecting the fact that national security remains the sole responsibility of each Member State in accordance with Article 4(2) of the TEU. An agreement was recently reached on **criteria representing a shared understanding** among the law enforcement authorities of the EU Member States on when a person should be regarded as a potential terrorist or violent extremist threat *('Gefährder')*[4]. The criteria are strictly non-binding and do not affect the mechanisms and procedures already established at European and national level. Their goal is to encourage the Member States to enter data on such individuals into the European databases and information systems, subject to the legal requirements governing these systems.

While the number of asylum seekers and refugees involved in terrorism and violent extremism remains very limited, terrorist attacks in Europe have triggered a debate on how to better prevent future attacks (see the June 2022 Council Conclusions on 'Protecting Europeans from terrorism: achievements and next steps'[5]). The Presidency has made efforts to **strengthen cooperation and exchange of information between immigration and asylum authorities and between CT authorities at European level, and CT and immigration and asylum authorities at national level,** in accordance with their respective competences, on foreigners who intend to stay on EU territory and may pose a terrorist threat. **Central points of contact, building on Member States' existing network structures, can further facilitate international cooperation and information exchange.** In addition, a **compendium** is being prepared with an overview of existing national procedures, working structures and consultation mechanisms within the Member States[6].

---

3 Council Conclusions on Internal Security and European Police Partnership (13083/1/20 REV 1).
4 9988/24.
5 9997/22.
6 6146/24.

Online terrorist and violent extremist content accentuates risks of polarisation and radicalisation and augments the risk of a potential spillover from conflicts[7]. **It is crucial to continue addressing and acting against the spread of violent extremist and terrorist content online by ensuring the full implementation and use of the Regulation on addressing the dissemination of terrorist content online (TCO Regulation)[8] [9]** and the Digital Services Act (DSA)[10]. For this reason, the Presidency, in the TWP, conducted a **discussion on the main gaps in and obstacles to the application of the TCO Regulation**, including any types of content and providers not sufficiently regulated, which should feed into the evaluation of the legislation already in place and potential amendments.

Despite progress, the **lack of sufficient content moderation** by some platforms is worrying and requires more engagement, in particular from the internet industry. The larger platforms have become better at moderation, but their efforts remain insufficient while new, smaller platforms, with minimal or no moderation, are proliferating. Content moderation in non-European languages is essential. The use of the PERCI[11] platform is strongly encouraged. In addition, voluntary efforts are valuable and should continue through the EU Internet Forum, including efforts to tackle the spread of terrorist and violent extremist content online, regardless of ideology, and to address borderline content (i.e. content that might be legal but is harmful) and emerging challenges related to new technologies, in particular the risks and opportunities associated with generative artificial intelligence.

PUBLIC

---

7 15443/23.

8 Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online (OJ L 172, 17.5.2021, p. 79).

9 Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online (OJ L 172, 17.5.2021, p. 79 and 6677/24 + ADD 1).

10 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (OJ L 277, 27.10.2022, p. 1), fully applicable since 17 February 2024.

11 Plateforme Européenne de Retraits de Contenus illégaux sur Internet (European platform for the removal of illegal content online).

Transnational links and the borderless online world create a **need to continue strengthening the dialogue with key third countries**. Cooperation with third countries should be further developed in accordance with national and EU legislation, in the form of cooperation between the competent internal and external security actors, with a view, in particular, to sharing CT experience, building CT capacities and preventing and countering violent extremism. Cooperation should also include the exchange of information on foreign terrorist fighters (FTFs) (which could be used in criminal proceedings, e.g. regarding travel, possible returns, and networks facilitating travel by FTFs).

Climate change and environmental concerns triggering the radicalisation of violent extremists and terrorists is an emerging phenomenon in the EU that requires further attention. While, in most cases, the actions of such individuals are more an issue of public order and civil obedience (vandalism, damaging buildings, blocking access to roads, infrastructure etc., but not violence against people), new forms of protest have been observed. Climate activism is on the rise, together with an increased willingness to use violence, marking a shift from environmental activism to **environmental extremism**[12]. For this reason, the Presidency has taken steps to obtain a better understanding and overview of this problem. The expression of environmental concerns in terrorist and violent extremist discourse online should be addressed through existing instruments, such as the EU Internet Forum and the EU Internet Referral Unit at Europol.

Potential new forms of violent extremism not attributable to specific ideologies, often based on conspiracy narratives and sometimes fuelled by foreign state actors, are assessed to be of concern and should be closely monitored. The threat posed by violent extremism and terrorism is constantly evolving, broad and complex, which makes dialogue with key third countries and relevant international organisations increasingly important. Countering violent extremism and terrorism has been an important theme in the recent meetings of the EU-US Dialogue on Justice and Home Affairs and the EU-UK Counter-Terrorism Dialogue.

The Presidency invites Ministers to take note of the above.

---

[12] 5982/24: EU CTC paper on 'The role of climate change and environmental concerns in violent extremist and terrorist radicalisation in the EU'.