Non-paper – Countering together: Fighting Online Radicalisation, Violent Extremism and Terrorism

By Germany, France and the Netherlands – December 2025

The online world is an integral part of our lives and offers unprecedented opportunities for communication, innovation, and access to information. At the same time, this digital space presents risks to the internal security of the European Union. Violent extremist and terrorist groups exploit online platforms to spread and sustain propaganda, recruit new members, and even plan attacks. In recent years, we have observed a concerning trend where minors and young people are increasingly becoming involved in terrorism and violent extremism.[1] The online domain plays a significant role in the radicalisation of these minors and demands our focused attention.

In recent years, significant progress has been made within the EU to address these challenges, including through the adoption of the Terrorist Content Online Regulation (TCO) and the Digital Services Act (DSA). In relation to the protection of minors, we also welcome the recently published guidelines for Article 28 of the DSA. Despite the progress that has been made, we observe that the problem of online radicalisation is increasing, especially where it concerns minors. This requires further action. It is important to clearly distinguish between terrorist content and violent extremist content. Terrorist content is illegal under EU law and is addressed through binding measures such as the TCO Regulation. Violent extremist content, while not illegal, can nonetheless foster radicalisation processes that may lead to terrorism. It therefore calls for voluntary and proportionate measures to reduce its impact.

When it comes to tackling online radicalisation, violent extremism and terrorism, it is crucial to safeguard fundamental rights such as freedom of expression, respect for private life and communication, and the protection of personal data. In this light, this non-paper emphasises that violent extremist content may pose significant risks that warrant appropriate measures albeit making sure it is not treated in the same fashion as illegal content. Freedom and security are not opposites, but they do demand constant consideration and vigilance to ensure the internet remains a space where fundamental rights are protected and abuse is effectively addressed. Through this non-paper, Germany, France and the Netherlands intend to outline possible next steps to address online radicalisation, violent extremism and terrorism, while also respecting fundamental rights online.

[1] Europol, European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg, 2025.

Key takeaways

- **Fundamental rights**, including the right to freedom of expression and the right to privacy, should be central to the approach of the European Union to address online radicalisation, violent extremism and terrorism.
- The current threat picture necessitates **additional action** to counter online radicalisation, violent extremism and terrorism, especially where it concerns minors.
- We call for a **Code of Conduct** that is **co-regulatory**: it is important to involve Member States, online platforms, civil society as well as experts with technical expertise.
- This code of conduct should include **key elements** regarding user empowerment, strengthened sharing of signals, addressing platform migration and systemic risks.
- We encourage exploring the potential to expand the **'Lantern Project'** from its focus on Child Sexual Abuse Material (CSAM) to include Terrorist and Violent Extremist Content (TVEC).
- This non-paper emphasizes that 'harmful yet legal' content should not be addressed in the same manner as illegal content. Most of the measures outlined below are **not solely focused on content.**

Addressing the role of online platforms through a Code of Conduct

The current threat landscape highlights the need for further action to support the effective implementation of the DSA in addressing the risks stemming from online radicalisation. Online platforms wield significant influence over the online public space and thus bear a profound responsibility to ensure a safe and secure environment for their users. Therefore, there is a growing imperative to take this responsibility more seriously and take further action. We therefore invite the European Commission to initiate the establishment of a Code of Conduct to address online radicalisation, violent extremism and terrorism. Indeed, it should be noted that Codes of Conduct represent a relevant tool under the DSA, including as an appropriate mitigating measure against systemic risks for very large online platforms (Article 45 of the DSA). The appropriate regulatory burden for online platforms must be carefully considered in the development of the Code of Conduct. To encourage online platforms to adhere to this Code of Conduct and ensure all relevant voices are taken into account, it should be co-regulatory. The European Commission should establish strong incentive measures to ensure broad endorsement of the new Code of Conduct, notably by online platforms that are abused for violent extremist and terrorist purposes. In that light the Code of Conduct could contain commitments in the following areas.

Reinforcing the protection of users

This Code of Conduct should include more stringent measures that platforms can implement to protect their users and offer clear guidance to platforms on how to comply with these measures. The guidelines for Article 28 of the DSA offer strong examples, some of which could be broadened to apply not only to minors but also to adult users. An example can be found in Section 6.5.2 on user control and empowerment, which includes measures such as allowing users to reset recommended feeds and providing explanations for why specific content was

recommended to them. Additionally, measures to better protect users could include media literacy initiatives and tools to strengthen critical thinking, such as providing context for visible content or offering guidance on how to assess online information. Online platforms could also implement safe design practices to ensure the legality and safety of their algorithms and reduce the risk of individuals attempting to recruit users for terrorist or violent extremist activities (pursuing safety by design).

Enhancing online prevention efforts

Online platforms could increase the visibility of online prevention efforts, building on successful past initiatives. This may be achieved by modifications of news feed algorithms and could include collaborative approaches between online platforms, civil society, and governments, such as redirecting users searching for violent extremist content toward appropriate counter-narratives or civil society interventions. Counter-narratives must always be evidence-based, co-designed with trusted local actors, and regularly evaluated. Moreover, these programs can help identify vulnerable online users and refer them to P/CVE practitioners for targeted support.

Strengthening the sharing of signals of online radicalisation

Whilst recognising that online platforms operate in a different context from offline actors, it would be important to encourage online platforms to share clear warning signals that come to their attention with competent national authorities in a secure manner, while fully respecting privacy standards and data protection requirements. Authorities would then assess the validity of the signals and whether these warrant further action or meet the relevant legal criteria. Such an approach would not require platforms to police content or behaviour, but rather to be committed to act as responsible partners in identifying and passing on concerning signals at an early stage, mirroring practices that have already proven effective offline.

Addressing platform migration and repeat offenders

Violent extremist groups frequently cast their net on mainstream platforms, using their broad reach and large user base to attract attention. Once caught in it, an interested user is then steered away toward online spaces with little or non-existent content moderation where recruitment can take place largely beyond the view of authorities. This form of 'platform migration' plays a crucial role in the life-cycle of online violent extremist networks, ensuring their continued presence across various platforms despite content moderation efforts. Platform migration has thereby become a deliberate tactic used by violent extremist groups to exploit the online ecosystem, circumvent content moderation efforts, and ensure the persistence and longevity of their online presence. In addition, platform migration further complicates efforts by law enforcement to take action. As such, platform migration exemplifies the complex challenges posed by online terrorism and violent extremism. It highlights the cross-platform nature of the problem and underscores the shared responsibility of all stakeholders in addressing it.

In response, we encourage exploring the potential to expand the 'Lantern Project' from its focus on Child Sexual Abuse Material (CSAM) to include Terrorist and Violent Extremist Content (TVEC). Lantern is a cross-platform signal sharing program for companies to strengthen how they enforce their child safety policies. This initiative offers a solution by enabling tech companies to securely share signals about potentially harmful or abusive users. Lantern thus provides a solution for online platforms to overcome current limitations to cross-platform collaboration. We also call upon online platforms to share and implement best practices for countering platform migration, such as the use of human content moderators who actively monitor and follow up on outlinks to other online platforms, as some online platforms already do. The EU Internet Forum would be an ideal platform for sharing these best practices. Finally, coordinated take-down procedures should be established so that specific violent extremist networks can be targeted across multiple online platforms, ensuring that their content is systematically and simultaneously removed.

Explicitly assessing violent extremism under existing systemic risks

The DSA currently outlines four categories of systemic risks. Notably, it includes the actual or foreseeable negative effects on democratic processes, civic discourse, electoral processes, as well as public security and the actual and foreseeable negative effect on the protection of public health or of minors. When assessing such systemic risks, providers should also explicitly focus on how their services can be abused for the dissemination of violent extremist content that may not be illegal but contributes to the aforementioned systemic risks. In particular, they should consider risks arising from the design and functioning of their systems that have an actual or foreseeable negative effect on the protection of minors (Article 34 of the DSA), who are especially vulnerable to algorithmic entrapment and filter bubbles. This means that online platforms should adopt risk mitigating measures to limit the spread of violent extremist content on their platforms. This does not entail equating such content with illegal content, nor requesting that such material be deleted, but rather acknowledges the inherent risks it poses and supports additional action to address these risks. France, Germany and the Netherlands call upon the European Board for Digital Services, in cooperation with the European Commission, to include in their annual reports on the most prominent and recurrent systemic risks, as described in Article 35 of the Digital Services Act, the identification and assessment of risks pertaining to the spread of violent extremist content on online platforms. This would represent a concrete step toward strengthening the EU's collective ability to safeguard democratic processes from the threats posed by violent extremist content.

<u>Next steps</u>

The European Commission is invited to include a proposed Code of Conduct on fighting online radicalisation, violent extremism and terrorism in the new EU Agenda on preventing and countering terrorism and violent extremism. The European Commission could establish dedicated expert groups to build common ground on the outline of a new code of conduct. It is important that Member States, online platforms, civil society as well as experts with technical expertise are represented in these expert groups. The resulting Code of Conduct should

follow a co-regulatory approach and ensure that fundamental rights, including the right to freedom of expression, remain central in addressing online radicalisation, violent extremism and terrorism.