Council of the European Union

Brussels, 20 June 2025
(OR. en)

10394/25

LIMITE

CT 77
ENFOPOL 215
COTER 99
JAI 864
EUROPOL

NOTE

From:	Presidency
To:	Terrorism Working Party (TWP)
Subject:	Exploitation of new technologies for extremist and terrorist purposes

I. The New Technologies threat to the security of the EU

Security and law enforcement agencies face growing challenges due to the exploitation of modern technologies by terrorist and extremist organisations. These innovative tools can support various aspects of radical group operations — from enabling illicit financing and secure communication channels to facilitating the execution of terrorist attacks. Particular attention is given by authorities to technologies such as 3D printing, CBRN-E, unmanned aerial vehicles (UAVs), encrypted communication platforms, blockchain (including cryptocurrencies), artificial intelligence (AI), and the metaverse. At the same time, these technologies can be leveraged by states to detect, prevent, and mitigate emerging threats.

This document aims to facilitate comprehensive stocktaking and structured CT information exchange within the Working Group Community on threats posed by the malicious use of emerging and disruptive technologies. It serves as a platform for Member States and relevant stakeholders to share insights, recent developments, case studies, and assessments of how such technologies are being exploited by terrorist and extremist actors. Furthermore, the document calls for strengthening the sharing of CT-related best practices, innovative countermeasures, and strategic responses developed at national and EU levels. It seeks to enhance collective situational awareness and operational preparedness, and to contribute to the formulation of more effective and coordinated policy approaches to counter these evolving risks.

1. Artificial Intelligence (AI)

Counterterrorism (CT) is undergoing a significant transformation due to the ongoing technological developments and, in particular, the use of artificial intelligence (AI) technology. This technology poses significant risks when misused by terrorists, who exploit AI for propaganda, recruitment, and behavioural manipulation, creating challenges for CT authorities. On the other hand, this technological advancement has led to substantial improvements in crucial areas such as the prevention of radicalisation, threat detection, data analysis, surveillance, and intelligence gathering. AI systems, particularly generative models such as large language models (LLMs) like ChatGPT, image and video generators, and voice synthesizers, allow for rapid processing of vast datasets, identification of patterns, and targeted interventions for preventing and countering violent extremism (P/CVE). For example, AI-powered tools have the capacity to analyse social media content in order to support content moderation efforts, detect extremist and terrorism-related content, predict potential threats, and support law enforcement in real-time decision-making. Effective and consistent use of these tools is critical for countering online radicalisation, as they enable authorities to monitor and respond to emerging threats efficiently.

The AI Act

The AI Act[1], which was adopted on 13 June 2024 and entered into force in August 2024[2], is the first comprehensive legal framework for AI. While some parts are already applicable, others will be in the near future.[3] The AI Act contains several key provisions that will have an impact on how and under which safeguards AI based systems and functionalities may be used in the Justice and Home Affairs (JHA) domain. Using the concept of the risk-based approach built into the proposal will mean that some use cases specific to law enforcement, border management and migration are placed under the "high-risk" category or entirely prohibited. This would include core use cases such as real-time remote biometric identification, categorisation based on biometric data, predictive policing, and risk assessment, which are all instrumental tools in law enforcement and other competent authorities' toolbox, as we move further into smarter and more digital policing.

---

1 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 (Artificial Intelligence Act).

2 The regulation entered into force in 2024, with a general date of application of 2 August 2026.

3 The definition of an AI system as a machine-based system designed to operate with varying levels of autonomy is provided, and it is further explained that such systems are capable of generating outputs such as predictions, content, recommendations, or decisions that influence physical or virtual environments. The Act places significant emphasis on the principles of safety, transparency, and respect for fundamental rights, requiring providers to label AI-generated content in a machine-readable format and inform users when interacting with AI systems.

Challenges of Generative AI

The capacity of generative AI to generate text, images, audio, and video on a large scale carries considerable risks. Terrorists often exploit open-source models, which are frequently stripped off safety features, in order to produce propaganda, translations, deepfakes, and memes that serve to amplify disinformation, social polarisation, and extremist messaging. The June 2024 paper by the International Centre for Counter-Terrorism (ICCT) highlights growing interest among terrorist groups such as Al-Qaeda, ISIS, and Hezbollah in using AI to expand their propaganda and global influence. For instance, Da'esh published in 2023 a tech guide on the secure use of generative AI tools, while some far-right groups produced a "guide to memetic warfare" with AI-generated extremist content. Europol has observed an increase in the use of AI-driven ideological narratives, including interactive historical or fictional characters, which bypass online moderation by service providers. These tools enable terrorist organisations to target younger demographics with visually appealing and emotionally charged content, thereby increasing the reach and impact of extremist messaging.

EU Measures

The AI Act and the Digital Services Act (DSA)[4] established a foundation for safe AI use that is complemented by the Regulation 2021/784 on Addressing the Dissemination of Terrorist Content Online (TCO Regulation), which has significantly helped to reduce the availability of terrorist content online. The DSA is a legislative instrument that was designed to address the issue of illegal content amplification by recommender algorithms. The DSA also tackles societal risks such as disinformation. Apart from the legislation, tools to promote voluntary cooperation with the industry were also put in place such as the EU Internet Forum (EUIF), which has a particular focus on the issue of malicious online content, and a source undertaken in December 2023 confirmed the amplification of terrorist and extremist material by algorithms across a variety of platforms. Finally, Europol provides support to Member States via the EU Platform to Combat Illicit Content Online (PERCI), facilitating referrals and removal orders for terrorist content in accordance with the TCO Regulation. The EU funds AI related research through the Horizon and Internal Security Fund (ISF) programmes, which helps develop fundamental rights-compliant tools for law enforcement. The EU Innovation Hub for Internal Security coordinates AI capabilities, while the EU Security Data Space for Innovation (EU SDSI) is being developed to enhance data-driven CT efforts.

Way Forward

In order to combat the misuse of AI, a robust collaboration is required between policymakers, law enforcement, industry, civil society, and academia. Focus should be placed on:

- Conducting in-depth research[5] on the role of artificial intelligence in the dissemination of terrorist propaganda and its societal impact. Research is instrumental in enhancing the AI and policing capabilities for law enforcement, including training and cutting-edge tools, while ensuring compliance with fundamental rights.

- The development of AI has a significant impact on EU industry and sovereignty. Consequently, it is crucial to invest more in this domain to support European companies, including start-ups, as well as research and innovation in the field of internal security.

---

4 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).

5 There is also research by Vox-Pol (such as voxpol.eu/wp-content/uploads/2024/04/DCUPN0254-Vox-Pol-AI-Extremism-WEB-240424.pdf

- Strengthening international cooperation to address cross-border AI misuse, including sharing best practices and intelligence is a very important step in addressing the issue[6].

2. EU CBRN-E threat

The EU faces a growing concern over CBRN-E (Chemical, Biological, Radiological, Nuclear, and Explosives) threats and incidents, including both accidental events and intentional misuse (e.g. terrorism or sabotage).

The nature of these threats include:

- possible use of toxic industrial chemicals (e.g., chlorine), warfare agents (e.g. sarin), and nerve agents
- potential use of pathogens (e.g. anthrax, ricin), pandemics, or bioengineered agents
- there is a radiological/nuclear-related risk of dirty bombs (RDDs), theft of radioactive sources, or attacks on nuclear facilities.
- manufacturing of IEDs, homemade explosives, and misuse of dual-use materials.

Incidents in the EU regarding CBRN-E have centre, among others, on:

- Salisbury (UK, 2018): Nerve agent attack (Novichok) targeting former Russian spy.
- Brussels (2016): Terrorists linked to the Paris attacks, who were reportedly researching a nuclear facility in Belgium.
- Anthrax hoaxes: Numerous false alarms and suspicious white powder letters
- Explosives: Regular dismantling of illegal bomb-making operations and seizure of explosive precursors

---

6 The Global Internet Forum to Counter Terrorism (GIFCT) has established Year Five Working Groups to address online terrorist and extremist content.

The 2017 EU CBRN Action Plan addresses chemical, biological, radiological, and nuclear risks through an all-hazards approach, promoting cross-border and cross-sectoral cooperation. The four objectives of the programme include: reducing accessibility to CBRN materials**,** enhancing preparedness and response to CBRN incidents, building stronger internal and external partnerships with regional and international actors, and improving knowledge of CBRN risks through research and analysis.

Most of the 30 actions have been implemented, including the establishment of a CBRN Security Advisory Group for information sharing, coordination, and joint activities among Member States.

Significant developments, including the COVID-19 pandemic, Russia's 2022 invasion of Ukraine, and institutional changes such as the Health Emergency Preparedness and Response Authority (HERA) and the rescEU initiative, necessitate a comprehensive revision of the Action Plan. The ProtectEU European Internal Security Strategy presented earlier this year, announced that in 2026 the Commission will adopt a new CBRN Preparedness and Response Action Plan. The revision will address emerging risks, such as evolving CBRN threats and technological advancements (such as the abuse of AI for creation or enhancement of chemical or biological agents or for facilitation of IEDs development), in order to ensure a robust framework.

3. 3D Printing

Emerging Threat

The process of additive manufacturing, otherwise referred to as 3D printing, has been identified as a potential security risk due to its capacity for illegal firearms production. The EU Action Plan on Firearms Trafficking (2020-2025) and Europol's 2023 Terrorism Situation and Trend Report (TE-SAT) both highlight an increasing interest in 3D-printed weapons, particularly among right-wing extremists. Affordable 3D-printing technology and widely available online blueprints, counting with the support of AI to improve the level of perfection of those blueprints, while getting rid of manufacturing issues whilst printing components, exacerbate the threat by enabling individuals to produce firearms or components with only minimal regulation.

State of Play

Seizures of 3D-printed weapons in the EU are limited, often involving experimental or hybrid models combining plastic components with unregulated metal elements, such as steel tubing or springs. Notable cases include:

- **Germany (2019)**: A lone actor attacked a synagogue in Halle, using homemade firearms with 3D-printed parts, driven by anti-Semitic and anti-feminist ideologies.
- **Netherlands (2022)**: Authorities arrested an individual for manufacturing a partially 3D-printed FGC-9 semiautomatic rifle, linked to incitement and terrorist crimes.
- **Slovakia (2022)**: An individual adhering to accelerationist ideologies shared instructions for 3D-printing firearms online and was in contact with attacker in Bratislava.
- **Iceland (2022)**: A foiled right-wing terrorist attack involved two individuals who produced partially 3D-printed FGC-9 weapons which they intend to sell in order to finance their plans.

Hybrid weapons, combining 3D-printed parts with metal components, pose the greatest threat as metallic 3D printing becomes more accessible and affordable.

Legal Framework

The Firearms Directive 2021/555 regulates all firearms, including 3D-printed firearms, under categories A (prohibited), B (subject to authorisation), and C (subject to declaration). However, it does not address digital blueprints. The Commission's report on the Directive acknowledges the potential threat posed by affordable 3D-printing and online blueprints, particularly for hybrid weapons. It suggests regulating blueprint possession, publicity, and distribution to prevent illicit manufacturing.

Way Forward

- Assess criminal sanctions for the illicit manufacture of 3D-printed weapons across Member States, ensuring they are effective and proportionate
- Establish specific rules for the acquisition, possession, and distribution of 3D-printing blueprints
- Collaborate with the 3D-printing industry to implement technical limits and regulate blueprint access, thereby reducing the risk of misuse

4. UAVs/Drones

The latest information on the threat landscape related to the use of UAVs, in particular drones, stemming from the war in Ukraine and the Middle East underscores a significant evolution in the methodology of terrorist operations, highlighting the potential for using drones to be exploited for malicious purposes. The daily performance gains in drone technology systems in terms of flight speed and duration, payload capability, integration with AI for autonomy and swarming capabilities, independent 3D printing, modularity of components, and resistance to countermeasures is constantly changing the landscape[7]. Europol's 2023 TE-SAT report predicts an increase in accessibility, with drones being traded anonymously online or combined with CBRN materials, posing significant risks. The Counter-Terrorism Committee of the UN Security Council emphasises the need to understand terrorist drone acquisition and use to develop effective countermeasures. The Commission communication ProtectEU – a European Internal Security Strategy adopted on the 01 April 2025 is referring to the increasing security challenge posed by drones and to some of the key actions of the EC Communication while the new EU agenda on preventing and countering terrorism and violent extremism will include the ongoing and future strands of work to counter the threat posed by non-cooperative drones.

Preventive Measures

The Commission adopted on 18 October 2023 a communication on countering potential threats posed by drones as a flagship action of the drone strategy 2.0 (November 2022). The Communication identifies18 key actions, aiming towards putting forward a comprehensive fully-fledged EU counter-drone policy. Among the actions already implemented, the set-up of a C-UAS expert group, the release of technical handbooks, the development of a digital platform containing information on drone incident, the development of training for the use of C-UAS for law enforcement, the allocation of funds in the contest of the Protect Call 2024 to a project focusing on C-UAS. Ongoing work to implement a harmonised testing methodology for counter drone system, the development of voluntary performance requirements for C-UAS and the upgrade of the JRC counter drone living lab into a Centre of Excellence. In addition, a thematic cluster within the EU Innovation Hub for Internal Security was established at the beginning of 2025 under the lead of Frontex to better coordinate capabilities on UAVs.

---

[7] For the time being no terrorist attacks have been recorded in the EU performed with the use of drones. The daily performance gains in drone technology systems represent an increasing threat that could affect our internal security.

5. The metaverse

The metaverse, a network of 3D virtual worlds powered by virtual reality and AI, is primarily used for gaming but has potential for broader applications. Its immersive nature poses significant terrorism risks, including recruitment, propaganda, financing, training, and attacks, with real-world psychological and societal consequences.

The metaverse's immersive environment, engaging all five senses, enhances propaganda and emotional manipulation. Additionally, the metaverse has become a fertile ground for phishing, social engineering, and Non Fungible Tokens (NFTs) scams[8]. Attackers use fake avatars and websites to deceive users into revealing sensitive information or authorizing malicious transactions, leading to substantial financial losses. Furthermore, avatars can spread extremist ideologies, and terrorist groups may create virtual spaces, such as a "virtual caliphate," to radicalize and recruit. The emotional intensity could weaken users' alertness, increasing their vulnerability.

Metaverse platforms are increasingly incorporating encryption technologies[9] to safeguard user data and communications within virtual worlds. End-to-end encryption, along with other security measures, helps protect sensitive information, prevent unauthorised access, and ensure data integrity. Intelligence services will find it increasingly difficult to detect violent terrorists and extremists or radicalised individuals in this new encrypted online environment before they take action offline. The use of cryptocurrencies and other digital assets such as NFTs within the metaverse enables money laundering and anonymous funding of illicit activities. The decentralised nature of these transactions complicates efforts to trace and regulate financial flows.

Cryptocurrencies and non-fungible tokens (NFTs) enable anonymous terrorist financing. For example, terrorist groups could sell NFTs (e.g., swastikas, other terrorist symbols) or host virtual events to raise funds: their decentralised platforms make it more difficult to trace them. NFTs can also be used to store and spread violent extremist and terrorist content. They are particularly challenging as it is practically impossible to remove them from the Internet.

---

8 https://www.europarl.europa.eu/cmsdata/268589/eprs-briefing-metaverse_EN.pdf

9 Encryption is posing a risk to cyber security, as encryption has been designed to protect cyber security - which is recognised in several EU legal acts.

The metaverse supports combat training (e.g. shooting and precision shooting, hostage scenarios) and attack planning by replicating real-world targets, based on online maps or blueprints available online, including parliaments and schools. Its immersive simulations offer more than video games do, thereby, offering a safer training environment for terrorists.

Virtual events or spaces (e.g., concerts, gatherings) could be attacked, with acts such as avatar mass killings causing psychological harm and real-world repercussions.

EU Reflections

Europol's Innovation Lab and the EU Internet Referral Unit (EU IRU) are exploring the implications of the metaverse for law enforcement, including the policing of virtual spaces and the use of the metaverse for real-time investigative collaboration. The EU Counter-Terrorism Coordinator raised the risks of the use of the metaverse in the context of the fight against terrorism[10]. The GSC Analysis and Research Team's recent paper outlines key challenges and opportunities, emphasising the need for coordinated EU action. The European Clearing Board (EuCB) at Europol is looking into policing and investigative applications of the metaverse.

6. Crowdfunding, fundraising and cryptocurrencies

The use of crowdfunding, fundraising and cryptocurrencies for hybrid, terrorist, and extremist purposes is an emerging security concern. It is known that extremist and terrorist groups exploit online crowdfunding platforms to get funds under false pretences (e.g. charity, disaster relief).

Terrorist networks also use decentralized, peer-to-peer funding to bypass traditional banking oversight and to mobilize support across borders by appealing to ideological supporters. They tend to target niche audiences on alternative platforms with fewer controls (e.g. fringe social media).

Cryptocurrencies such as Bitcoin, Monero, or Ethereum are used to transfer money anonymously across jurisdictions. The scheme is exploited to evade sanctions and anti-money laundering regulations and to store value discreetly (e.g., in cold wallets).

Crypto-assets are used to fund operations, propaganda, or recruitment.

---

[10] 9292/22

Non-state actors use the aforementioned tools in non-kinetic domains as part of their hybrid activity. Cases include: funding cyberattacks or disinformation campaigns, supporting proxy groups in geopolitical conflicts, blending political extremism with cybercrime and financial fraud. They pose serious challenges as a result of the anonymity and lack of regulation in some jurisdictions but also because of difficulties in tracking fragmented microtransactions. There are also serious limitations to cross-border cooperation.

EU institutions like Europol, or global money laundering and terrorist financing entities like FATF, and national agencies are, in collaboration with the financial sector, increasingly monitoring blockchain transactions, tightening "Know your Customer /Anti-Money Laundering (KYC/AML) rules", and developing AI-based tracking tools. The EU Internet Forum further addresses financing activities of terrorist and violent extremist online.

II. Conclusion

Terrorist and extremist groups increasingly leverage of modern technologies, is posing significant challenges for security services. These technologies can facilitate illegal financing, secure communications, and terrorist attacks. Key tools include 3D printing, unmanned aerial vehicles (UAVs), encrypted communication platforms, blockchain technology (cryptocurrency and NFTs), and Artificial Intelligence (AI).

3D printing enables the production of weapons and components, with knowledge accessible on the darkweb and online forums. While global use remains limited, it is growing. In Poland, cases of 3D-printed firearms are isolated, likely due to restricted firearm access.

UAVs are potential terrorist tools due to their affordability and availability. They can serve as weapon platforms or missiles, with tactics from conflicts such as the Russia-Ukraine war being studied by terrorist groups for future attacks.

Encrypted messaging applications (e.g. WhatsApp, Signal, and Telegram) and social/gaming platforms enable anonymous communication, and facilitate the spread of propaganda, and disinformation by terrorist and violent extremist actors. The volume of real-time data and encryption advancements is a challenge for security services, calling for further action at EU level. In that regard, the Commission announced in the communication "ProtectEU: a European Internal Security Strategy" the preparation of a technology roadmap on encryption to identify and assess technological solutions that would enable law enforcement authorities to access encrypted data in a lawful manner, safeguarding cybersecurity and fundamental rights.

Cryptocurrency and crowdfunding platforms offer partial anonymity, making them attractive for terrorist financing. In Poland, extremist groups use online fundraising to support operations. Improved identification of transaction parties is critical in countering these activities.

AI enables the rapid creation and multilingual translation of propaganda, multiplying its reach. Large language models can also perform tasks that support extremist activities by using online resources.

Emerging technologies, including among others AI, 3D printing, drones, the metaverse as well as cryptocurrencies and crypto-assets, offer transformative opportunities for counterterrorism but also pose significant risks due to their potential for misuse. Although a lot has already been done at the EU framework level (i.e. TCO, DSA, AI Act) we must strengthen and foster collaboration with industry, and invest more in research, innovation, and law enforcement capabilities to address these threats. Coordinated action across policymakers, agencies, and private sectors is essential in order to stay ahead of technological advancements and to ensure a proactive response to the threat of terrorism.

III. Questions for Delegations:

1. Have Member States recently experienced violent extremist and/or terrorist incidents involving the misuse of new technologies (AI, metaverse, CBRN, cryptocurrencies, and UAVs)? Do Member Sates see an increase in the number of incidents involving the use of UAVs (e.g. air traffic, disturbances, flights over critical infrastructure and state facilities)?

2. Are Member States aware of any other modern technological tools that could be used in terrorist activities in the near future?

3. How is resilience to new technology threats being built? Are the security authorities and the law enforcement agencies of the Member States using new technologies to combat threats and to what extent, and in the framework of which initiatives or projects?