Council of the European Union

Brussels, 2 June 2022
(OR. en)

9292/22

LIMITE

CT 87
JAI 690
COSI 137
CATS 27
ENFOPOL 280
COPEN 198
DIGIT 102
TELECOM 231
HYBRID 45
CYBER 180
IND 182

NOTE

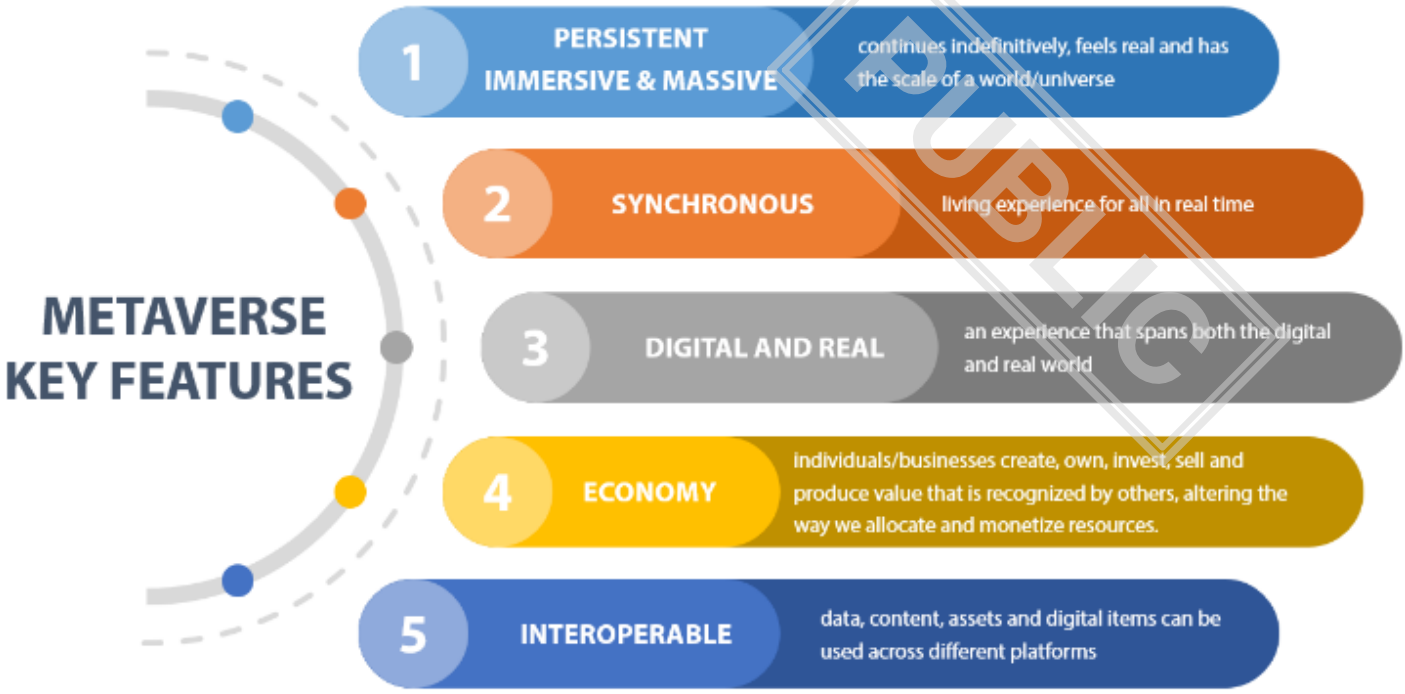
From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	The Metaverse in the context of the fight against terrorism

Introduction

The **Metaverse is a network of 3D virtual worlds focused on social connections,** based on the use of real capture tools, such as virtual reality headsets. As such, use of the Metaverse depends on a number of requirements, such as availability of hardware, a strong internet connection, accessibility and security, which currently prevent it from achieving its full potential. Yet while today the Metaverse is mainly used for gaming, in the future, it will also be used for a host of other activities in different contexts and is likely to play a greater role in people's lives.

The Metaverse could be a valuable part of life in the future. However, like any new technology, the Metaverse could also be misused for criminal purposes, including by terrorists. As such, it will encounter the same legislative and monitoring challenges as the internet in general, but in an even more pronounced way on account of its implications for human emotions.

Figure 1 Source: General Secretariat of the Council, Analysis and Research Team (ART) paper 'Metaverse – Virtual world, real challenges' 9 March 2022 (hyperlink in Fn 14)



All aspects of terrorism can be reinvented in the Metaverse, including recruitment, the spread of violent extremism, terrorist financing, training and the coordination of attacks. Ultimately, as a marketplace for entertainment and social interaction, the Metaverse itself can also become a target for terrorists.

Considering the field of digital possibilities that it opens up, we need to assess the challenges that could emerge from terrorist use of the Metaverse and the impact of the Metaverse on law enforcement. This paper will focus on **(I)** the specific modalities of the Metaverse in enabling radicalisation and recruitment, **(II)** the Metaverse as an enabler for real life, and **(III)** the Metaverse as a target. Recommendations on the way forward are included in the last part (**IV**). In the annex, there is a state of play of EU reflections on the Metaverse.

I. Specific modalities of the Metaverse in enabling radicalisation and recruitment

The Metaverse creates new challenges for counter-terrorism, different from those already raised by social media and previous technologies, given its much more immersive and emotional nature, with its creation of parallel worlds. Its specificities can lead to new threats and new ways of carrying out terrorist actions. At the same time, the Metaverse may also provide some opportunities for law enforcement, such as remote, real-time collaboration in criminal investigations.

A. Immersive Nature

The main feature of the Metaverse is its immersive dimension, with the creation of all-encompassing worlds where all five senses are used. In the coming years, technological developments will reinforce **this immersive dimension**, in particular by including other sensory captors, for example an olfactory one.[1] This may **weaken users' alertness and could ultimately lead to a higher level of vulnerability**.

B. Capture of emotions

Due to the intense emotional experience **offered by the Metaverse**, it could be difficult for some people to distinguish between real life and virtual reality, **heightening their emotional reactions**. **Conversely, the distinction between the person and the digital avatar could also lead to a dampening of emotions and underestimation of risks**: some users might believe that what is happening in the Metaverse is not real, even if there are real consequences for their lives. The importance of emotional manipulation in terrorist radicalisation is well known.[2]

1 *Olfaction in virtual reality video - Swiss Center For Affective Sciences - UNIGE*

2 *Hayward, KJ & Cottee, S 2011, 'Terrorist (e)motives: the existential attractions of terrorism', Studies in Conflict and Terrorism, vol. 34, no. 12, pp. 963-986.*

In addition to the Metaverse's capacity to alter emotions as such, data about users' emotions could be misused by terrorists.[3] The use of hardware such as helmets, glasses or other captors will soon make it possible to capture emotions and reactions in real time, **potentially enabling terrorists to manipulate people**. For example, it may become possible for terrorists to monitor what a person is looking at in the Metaverse, to learn what is attractive for him/her, to adapt their narrative accordingly, and then contact him/her by using his/her personal data. Terrorist groups might even be able to create their own Metaverse, where they can bring together people identified as sympathisers.

C. Use of avatars

Avatars and virtual representations, in particular, could be misused to stir up emotions and spread extremist ideology. Thus, historical, religious and ideological topics could be represented through avatars and the personalisation of appearances. Avatars could make it possible to feature deceased terrorist leaders in a virtual resurrection in order to galvanise supporters and encourage them to keep up their fight.

II. The Metaverse as an enabler for real life

A. Ideological (recruitment, propaganda, the Metaverse as a 'home' for extremists)

As seen above, the Metaverse can be used as a tool to spread ideology and contribute to radicalisation. In consequence, the Metaverse could **expand terrorist recruitment** with new attractive methods of propaganda**.** In an online environment where the emotional engagement is much stronger, **offline meetings could become less important than before**. Traditional job providers are already using the Metaverse to hire new staff,[4] terrorist groups could use it to find new recruits as well.

---

[3] According to a Stanford study, '*spending 20 minutes in a VR simulation leaves just under 2 million unique recordings of body language. Psychologists have never, in the decades of studying non-verbal behavior, had data sets of this magnitude*.' Protecting Nonverbal Data Tracked in Virtual Reality (stanfordvr.com)

[4] See for example https://www.beckershospitalreview.com/workforce/metaverse-opens-new-frontier-in-employee-recruitment-training.html

The Metaverse could also become a safe haven, where various forms of extremism are preached. This virtual world offers new possibilities for extremists to stay in touch with, and to exercise control over, a radicalised community through events and regular meetings. Extremist organisations could **create Metaverse spaces where they freely spread disinformation and hate speech, and where rejection of democracy brings people together.**

In the future, multiple Metaverse versions or Metaverse-like environments will emerge depending on investments and the products launched by companies such as Meta. This could lead to the emergence of **regional Metaverses**, linked to a State, company or community. Hence, the creation of a virtual caliphate or Da'esh base camp is one of the risks linked with this new world.

B. Financial (terrorist financing)

Blockchain technology and cryptocurrencies are building blocks of the functioning of the Metaverse. They enable the Metaverse to provide digital identification and proof of ownership, digital collection of assets (such as non-fungible tokens (NFT)) and crypto value transfer. In order to access the Metaverse, people will most likely be asked to own a cryptocurrency wallet to hold their digital assets. The Metaverse could therefore prompt an increase in their use.

However, there are growing concerns about the use of cryptocurrencies in terrorist financing,[5] due to the anonymity that they provide, the possibility of making instant payments and the ability to process cross-border transfers without any oversight from any authority or bank.[6] For example, crypto-assets could be used as a method for money laundering or fundraising. The main challenges linked to the use of cryptocurrencies are traceability, cooperation between decentralised financial actors, jurisdictional issues and, more broadly, the consequences of the development of a closed ecosystem.[7]

---

5 In 2020 the French anti-terrorist prosecutor's office noted an example of cryptocurrency being used to finance terrorism after the French security service (DGSI) conducted a preliminary investigation into a network that had been active since 2019. The network relied mainly on the purchase in France of cryptocurrency coupons, the references of which were transmitted by secure messaging to jihadists in Syria, then credited on bitcoin platforms

6 Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity - Chainalysis

7 General Secretariat of the Council of the EU, Analysis and Research Team (ART), "The crypto assets ecosystem. Suspicion, regulation, expansion?", 26 April 22, https://www.consilium.europa.eu/media/55832/crypto-assets-26-april-2022.pdf

Traceability of exchanges will be even more important in the Metaverse because of its strong links with cryptocurrencies. The rapid development of cryptocurrencies (more than 18 000 to date) makes monitoring very challenging.

One could imagine funds being raised through a sale of identity artefacts (swastikas, terrorist symbols etc...) in NFT, which are then used to customise avatars and display their affiliation to terrorist organisations. Various events could be organised by terrorist groups to **raise funds and strengthen their communities**, including online shows or avatar fights, which are already being staged in order to raise funds for right-wing violent extremism.

Such decentralised financing could help terrorist organisations develop their own online ecosystems and operate their own Metaverses (e.g., AQ or Da'esh Metaverse currency could be a marketing device).

C. Operational (training, attacks)

Virtual Reality (VR) is also used in the automotive industry to optimise production chains before their physical establishment.[8] The Metaverse is already used by some companies to give their employees combat training.[9] However, VR technology makes the Metaverse vulnerable to misuse by violent extremists and terrorists, who could use it to **provide and receive combat-relevant training** (including practice with precision shootings, tactics, hostage taking, and reconnaissance). The Metaverse could also offer a 'safer' training and simulation environment (without any risks of accidents with explosives, for example). **The emotional and immersive aspect of the Metaverse makes this kind of training more realistic and more absorbing**, surpassing the experiences obtained from video games. Training of this kind in a virtual world would be difficult to monitor, as it would not be linked to actual conflict and would not require travel to a conflict zone.

In addition, the Metaverse offers **new ways to coordinate, plan and execute acts of terrorism**.[10] Modelling can give terrorist organisations a tool to replicate targets from the real world (e.g. a parliament or a school) to practice a future attack and maximise its impact.

---

8 BMW uses Nvidia's Omniverse to build state-of-the-art factories | VentureBeat

9 Walmart gives employees VR combat training for holiday rush | ZDNet

10 The Metaverse offers a future full of potential – for terrorists and extremists, too - Iowa Capital Dispatch

The Metaverse can be **used as a platform for bypassing classical communication channels when preparing and organising attacks**. Terrorists could organise meetings, interactions, thrilling immersive experiences of an attack on police forces, a flow of images echoing people's grievances, and offer their own gaming space (e.g. Assassin's Creed-style for jihadists) in the Metaverse. Emotive historical events could be recreated in order to frighten users or galvanise supporters. For example, the destruction of Palmyra or major terrorist attacks (such as the destruction of the World Trade Center in New York or the attack at the Bataclan music venue in Paris) could be reproduced in virtual reality. Here, we find a similar issue as with social networks and video game chats.[11]

Indeed, video games could be viewed as a proto-Metaverse and should warn us about its possible negative use in the future.[12]

III. The Metaverse as a target

Terrorists could also find virtual targets in the Metaverse. Economic and social activities in the Metaverse will include the creation of "buildings" and the organisation of parties and events that could become virtual targets for terrorists, especially if these events support causes that they despise (such as gender equality or religious diversity). **These attacks can have repercussions in real life**.

Despite their virtual nature, attacks in the Metaverse have links with the actual world and therefore real consequences. For example, mass killings of avatars by terrorists (with bombings, beheadings, rape) could have psychological consequences.

IV. Recommendations for the way forward

The implications of the development of the Metaverse **should be closely monitored. It is important to address the risks early**.

11 ran_cn_conclusion_paper_videogames_15-17092020_en.pdf(europa.eu)

12 EU Counter-Terrorism Coordinator - ST 9066/20 Online gaming in the context of the fight against terrorism (pdf (europa.eu)

Although still under construction, the Metaverse holds the potential for violent extremists to exert influence in new ways through fear, threat and coercion. It could spawn a new area of terrorist activity that will bring fresh challenges to the availability of, and access to, data for use in criminal investigations and prosecutions. This new universe could also require updates of legislation. The authority that should monitor the development and use of the Metaverse is also an issue to be considered. It will be important to influence standard-setting in this area.

1. **A policy discussion in the relevant Council working parties** on the CT aspects of the Metaverse would be important for strategic direction. The Working Party on Terrorism (TWP) and the Standing Committee on Operational Cooperation on Internal Security (COSI) could be involved. A ministerial discussion could provide strategic direction.

2. An assessment could be considered of the adequacy of the **legal framework** for addressing the challenges the Metaverse may bring. This includes a review of the existing legal framework (e.g. how could the Terrorist Content Online (TCO) regulation, the Digital Services Act (DSA) and the Anti-Money Laundering and Countering Terrorist Financing (AML/CFT) legislation be applied to counteract some of the negative aspects of the Metaverse?) and potential future legislation. In addition, there may be a need to review the existing legal framework for accessing data by law enforcement authorities,[13] in case the Metaverse brings new categories of data beyond the 'traditional' ones (subscriber-traffic-content data).

3. Considering that we are still in the early stages of this phenomenon, it would be advisable to start **exchanges with Meta and other companies** in order to familiarise ourselves in detail with their intentions and safeguards regarding the Metaverse, especially on account of their interest in the European market. Engagement in the context of the **EU Internet Forum and in the context of EU-US dialogues** should also be envisaged. As a first step, it could be explored with Meta whether and how the aspect of financing in the Metaverse could be addressed in an EUIF workshop on fundraising activities online. The Global Counterterrorism Forum (GCTF) and the Global Internet Forum to Counter Terrorism (GIFCT), in which the technology industry participates, could address the issue as well.

---

[13] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

4. The EU Intelligence and Situation Centre **(EU INTCEN)** could be invited to report on the (potential) use of the Metaverse by terrorist groups.

5. The **EU Innovation Hub for Internal Security at Europol**, in collaboration with the **Europol Innovation Lab**, the **EU Internet Referral Unit** and **EC3 at Europol** should be encouraged to **continue exploring and addressing the terrorism and internal security risks** of the Metaverse. The practical implications of the Metaverse for law enforcement and justice in the context of investigations and prosecutions need to be explored with the support of Europol and Eurojust**,** including in the framework of the EU Innovation Hub for Internal Security.

6. **Influence standard-setting:** The Commission could be invited to raise law enforcement and judicial concerns concerning the technologies currently needed for the Metaverse in the various standardisation bodies in which it participates or with which it engages. Europol could consider becoming a member of the relevant standardisation bodies to support Member States in defending European law enforcements concerns. The Member States' law enforcement authorities should also be encouraged to participate. As with 5G, it will be important to reflect on how the EU's involvement and impact can best be leveraged and how it can be ensured that law enforcement and judicial concerns are taken into account. **The Metaverse does not appear to fit neatly into the mandate of any one standardisation body, so engagement with several actors should be considered**. These would include third countries, in particular like-minded, and industry bodies such as the Digital Living Network Alliance (DLNA) (founded in 2003 by several global companies with a vision of facilitating the sharing of photos, music, videos etc. among networks and devices), as well as, potentially, the Allseen Alliance, the Industrial Internet Consortium, the IoT Consortium, and the Open Internet Consortium.

7. It will be important to **further strengthen ongoing work**, particularly regarding the law enforcement aspects of the implementation of 5G; the identification, removal and amplification of terrorist content; encryption; and cryptocurrencies; and to **strengthen knowledge about the technologies that will underpin this Metaverse virtual network** (alternative communication and storage systems, blockchain, decentralised platforms, AR/VR etc.) and their implications for counter-terrorism.

State of play of EU reflections on the Metaverse

Given the many technological, legal and social implications of the Metaverse, the EU should not work in silos. Effective **coordination** of European actions in this area is necessary. **This implies strengthening analysis and initiatives to face this new challenge**, for which the EU is not yet prepared.

A number of EU actors have already started to reflect on the Metaverse, including on anticipating threats. For example, the GSC **Analysis and Research Team** recently published a paper that presents an overall description of the Metaverse while looking into some of the key potential challenges and opportunities.[14]

In addition, several projects have been launched. **Europol** has started to explore the law enforcement aspect of the Metaverse. The **Europol Innovation Lab**, through its Observatory function, will organise a workshop on the law enforcement implications of the Metaverse before the summer. This workshop should generate recommendations for future actions at Europol and in the Member States, which would then be published. In the context of Europol, **the European Clearing Board (EuCB)** is analysing the Metaverse.[15] **It is working on the Metaverse from two perspectives:** policing the Metaverse (e.g. should there be a police station in the Metaverse?) and using the Metaverse for collaborative, remote, real-time collaboration in criminal investigations. **The EU Internet Referral Unit (EU IRU)** is also working to better understand the implications of the underlying technologies (from the technical point of view, referrals, monitoring, etc.) in order to be ready when the Metaverse starts to be used by the general public.

---

[14] Paper of the Analysis and Research Team (ART) of the EU General Secretariat of the Council, Metaverse–Virtual world, Real challenges ART Paper 9 March 2022.pdf (consilium.eu.int)

[15] The EuCB is a structure consisting of a network of national points of contact (SPoCs), composed of innovation experts and investigators of the EU Member States' law enforcement agencies who regularly meet in the context of the Europol Innovation Lab to channel needs and operational requirements for technical solutions using new technologies from practitioners directly; doc 12859/20, The EU innovation hub and the innovation lab at Europol state of play