



SERIES ON PROTECTING DIGITAL SPACES

Concept Note

“Safeguarding the Metaverse: Countering Terrorism and Preventing Violent Extremism in Digital Space”

28 November 2022 9:00-11:00 am EST
Via Webex

1. Background

As the world becomes more and more interconnected and technology evolves rapidly, terrorists and violent extremists are also keeping pace by using electronic communication systems to recruit, radicalize, fundraise, plan and propagandize. Through its Series on Protecting Digital Spaces, the United Nations Office of Counter-Terrorism (UNOCT) has examined potential threats by not only looking at the use and misuse of Augmented Reality and Virtual Reality (AR/VR), but also at online video games and their adjacent platforms. These awareness-raising events have proven critical in bringing together different segments of society to gather evidence-based information on latest and emerging trends and offer guidance on safeguarding digital spaces in a gender-responsive and human rights compliant manner. Both initiatives placed a strong emphasis on the importance of whole-of-society and whole-of-government approaches to issues involving these technologies and platforms, while fostering collaboration and information sharing among law enforcement, academia, non-governmental organizations and the private sector.

UNOCT will continue leading the international response to the potential misuse of digital spaces by facilitating an expert panel on the next technological evolution: the metaverse. The idea for this technology was first conceptualized in the 1992 science fiction novel “Snow Crash” as a reality-based

virtual world accessible via goggles and earplugs, where users appear as avatars. Today, the metaverse is intended as a digital universe composed of several platforms characterized by the interaction of the virtual and physical world. The result of technological developments in the fields of blockchain, Artificial Intelligence, and Extended Reality (XR), an umbrella term referring to all immersive environments that merge the physical and virtual worlds, the metaverse will be a persistent and interactive experience composed of interconnected 3D environments that can be manipulated by the user and are accessible in real-time through immersive AR/VR technology. This is already generating an evolution in entertainment and digital social interaction, immersing the player in digitally designed environments through the manipulation of the optical and audible senses. Moreover, the metaverse will be based on the interoperability of data, allowing users to move digital assets and utilize them across multiple virtual spaces. This platform will be populated by virtual content and experiences that can engage with the real world. As a result, the metaverse is expected to revolutionize human engagement by facilitating social activities, learning and education, and means to conduct business.

As more aspects of everyday life are integrated into the metaverse, several features of this technology hold the potential to be exploited by terrorists and violent extremists. The ability to communicate narratives to audiences on an individual and personalized level will likely increase as this technology becomes more immersive, enhancing the capacity of terrorist and violent extremist groups to perpetuate extremist ideology in order to recruit and radicalize through reinforcing mechanisms such as the echo-chamber effect, groupthink, or gamification. Other risks are related to cryptocurrencies, which will likely be the main form of conducting commerce and business in the metaverse. Cryptocurrencies and Non-Fungible Tokens (NFTs) are digital currencies and assets maintained by a decentralized system using cryptography, rather than by a centralized authority, which makes it easier to disguise the source of funds, which is already attracting terrorist groups to use such platforms for financing and fundraising. Additionally, the metaverse will allow users to access hyper-realistic replications of real-world locations, potentially allowing terrorists and violent extremists to remotely access these areas for the purposes of planning, training, and coordinating attacks against vulnerable targets such as landmarks, tourist venues, entertainment venues, and religious sites.

By acting while the metaverse is still in its primary phases, governments and institutions working proactively and in coordination with relevant actors to develop adequate overview mechanisms, can reduce the possibility of terrorist misuse and to ensure interoperability, inclusiveness and safety in the metaverse while also protecting human rights and establishing clear governance standards. A whole-of-society approach with governments, civil society, academia, think tanks and private sector technology companies will allow UNOCT to keep abreast of the latest developments in technologies including AR/VR, online video games, and the metaverse, and their impacts on the everyday lives of members of the digital community. In addition to safeguarding the metaverse, CT and P/CVE practitioners can look to the metaverse as a means to conduct capacity-building activities and operations in innovative ways, such as through powerful storytelling which can be employed in efforts to counter violent extremist narratives and increase resilience to the presence of terrorists in digital spaces.

2. Methodology

This event aims at understanding the concept of the metaverse, as well as at raising awareness of and exchanging information on innovative and cutting-edge solutions. This should produce recommendations regarding preventing and countering potential terrorist threats and activity involving the metaverse, while also addressing current regulatory gaps at the intersection between State behaviour and corporate roles in the digital age. This is facilitated by tapping into the discussions, outcomes, and recommendations of previous events held during the Series on Protecting Digital Spaces, notably on the application of Augmented and Virtual Reality in CT and P/CVE work, and the use of Video Games by Violent Extremists and by furthering research and dialogue to include the metaverse. This expert panel event will bring together a geographically diverse and gender-balanced group of CT and P/CVE stakeholders from the public, private and technology sectors, civil society organizations, think tanks and academia, as well as leading innovators in the field of XR technologies and the metaverse.

During the first session, renowned experts on the metaverse will define and explain the concept of metaverse and the technology it incorporates, address its origins, current high levels of interest, and foreseeable developments, and discuss its role in today's society, emphasizing the opportunities this new technology provides. **In the second session**, the potential risks for misuse of the metaverse by terrorist groups and violent extremists will be explored and experts will discuss avenues to operationalize a multi-stakeholder approach for safeguarding the metaverse that is built on a clear, rights-compliant governance foundation. **Finally, in the third session**, counterterrorism (CT) stakeholders will analyze the opportunities of the metaverse for innovation in CT and P/CVE efforts in the digital era, leveraging on lessons learned by CT practitioners on other digital spaces such as online video gaming or AR/VR technology, and considering how these can be adapted to the metaverse environment. The United Nations through the UN Department of Political and Peacebuilding Affairs, as well as the United Nations Interregional Crime and Justice Research Institute (UNICRI), and the World Economic Forum through its initiative on Defining and Building the Metaverse, are increasingly turning towards immersive technology, by advancing research and facilitating discussion on this issue as well as by developing physical spaces in the metaverse aimed at enhancing peacebuilding efforts. Through its involvement in the initial phases of metaverse technology, UNOCT will be able to help facilitate safeguarding these digital spaces from misuse, as well as respecting human rights and the rule of law. Moreover, this event will facilitate cooperation between the public and private sectors, the information communications technology industry, civil society, research institutes, and academia groups by being a catalyst for continuous dialogue on this topic and providing recommendations that can help discussions in the space acting proactively and ahead of terrorist groups.

3. Main Objectives

- Serve as the first initiative to bring together relevant stakeholders, facilitate a discussion, and raise awareness on the potential impact of the metaverse on CT and P/CVE, using each stakeholder's comparative advantage and unique perspectives to strengthen the global response against terrorism and violent extremism.
- Keep abreast of the important developments in technologies including AR/VR, video games, and the metaverse, and their applicability in CT and P/CVE efforts.
- Showcase successful applications of AR/VR for CT and P/CVE purposes.
- Identify needs and challenges related to the metaverse, as well as the opportunities to develop new initiatives and tools on CT and P/CVE.

4. Expected Outcomes

- Position UNOCT to better inform beneficiaries and Member States on the potential presence of terrorists and violent extremists in the metaverse.
- Enhance the Office's partnerships with the private sector, technology, and ICT organizations through a proactive approach to safeguarding emerging technologies from potential threats, as well through consultations with all sectors of society.
- Gauge interest in the implementation of a working group for the metaverse as part of the upcoming Connect & Learn Community of Practice on Technology and ICT in CT and P/CVE.

5. Attendees

In line with UNOCT's commitment to a whole-of-society response to terrorism, the expert panels event will include representatives from the private sector, academia, think tanks, civil society, Member States, the World Economic Forum with the objective of strengthening alliances and partnerships.

6. Venue, Date, and Language

The roundtable will be conducted online via Webex, tentatively 28 November 2022, from 9:00 AM – 11:00 AM Eastern Time (ET, which is New York time). A link to the virtual launch will be sent to participants who have submitted their registration form. The event will be conducted in English. No interpretation will be provided.

7. Communication and Follow-up Actions

The event will be promoted on the social media channel through the @UN_OCT Twitter handle using the hashtags #UNiteToCounterTerrorism. The event will be live streamed on UN Web TV (webtv.un.org). A web story will be issued on the expert roundtable after the event on the UNOCT website (www.un.org/counterterrorism).

8. Focal Point

Ms. Leila Ezzarqui, Chief, External Partnerships Section (EPS), Special Projects and Innovation Branch, UNOCT (email: ezzarqui@un.org).