PERSPECTIVES ON TERRORISM

RESEARCH ARTICLE

The Metaverse and Terrorism: Threats and Challenges

Gabriel Weimann* and Roy Dimant

Issue XVII, Volume 2
June 2023

ISSN: 2334-3745

The metaverse is currently the leading hype in the digital world because of its seemingly infinite potential and possibilities. Large corporations are drawn to the metaverse because it appears as the cutting edge of digital and technological developments. The metaverse is presented by communication technology companies as the next Internet, a leap towards a universe of boundless, interconnected virtual communities. However, there are many potential risks and challenges that the metaverse raises, including technical, legal, security, business, tax, privacy, security, and users' well-being and safety (among many others). Cyber-savvy terrorists have been highly resourceful in adapting and applying online platforms and have taken advantage of every new development, platform, and application. Based on their past record, it is reasonable to assume that the metaverse is a new dimension that terrorists and violent extremists are poised to study, examine, and possibly utilise. This research article explores some potential uses of the metaverse by terrorists and suggests preemptive measures to minimise the risks of them doing so. If the advancement of the metaverse or similar developments is inevitable, we should consider risks and abuses and think more carefully about them when moving forward.

Keywords: Metaverse, terrorism, cybersecurity, virtual reality

*Corresponding author: Gabriel Weimann, Haifa University, email: weimann@soc.haifa.ac.il

Introduction

The term "metaverse," combining "meta" and "universe," was first introduced in the 1992 science fiction novel *Snow Crash*. The author, Neal Stephenson, used the term to describe a virtual reality-based advanced form of the Internet.[1] The metaverse presents an immersion of the physical and virtual worlds in the digital sphere, using 3D technologies and online communication devices like computers and smartphones, allowing people to have real-time interactions and experiences across long distances. The metaverse is presented by communication technology companies as the next Internet, a leap towards a universe of boundless, interconnected virtual communities where people can socialise, communicate, collaborate, enjoy remote concerts and performances, and buy and sell products using virtual reality devices. In 2021 Mark Zuckerberg presented his vision for the future:

> *In the metaverse, you'll be able to do almost anything you can imagine—get together with friends and family, work, learn, play, shop, create—as well as completely new experiences that don't really fit how we think about computers or phones today… In this future, you will be able to teleport instantly as a hologram to be at the office without a commute, at a concert with friends, or in your parents' living room to catch up. This will open up more opportunity no matter where you live.*[2]

The metaverse is currently the leading hype in the digital world because of its seemingly infinite potential and possibilities. Large corporations are drawn to the metaverse because it appears as the cutting edge of digital and technological developments. The underlying promise of a new universe where the physical and digital worlds can combine and bring together thousands of individuals is perceived as enhancing fundamental areas of daily life. Metaverse technologies have already been developed in online gaming. The *Second Life* virtual world platform of 2023 may be the first metaverse, which integrated many aspects of social media interactions into a three-dimensional world. Similarly, *Fortnite*, the computer game introduced in 2017, is based on a virtual battlefield where imaginary reality becomes real using metaverse technologies. *Roblox* is another metaverse platform where gamers can play user-generated games, based on virtual reality experiences. *Roblox* also allows users to buy virtual items and attend remote events, including concerts, mass ceremonies, and parties. But it is the wider range of uses and opportunities beyond gaming that make the metaverse so attractive in various domains such as education, commerce, politics, entertainment, communication, and social interaction.

Because of its immense potential in benefiting the digital communications world, many tech giants are already entering the world of the metaverse. Facebook changed its name to Meta, officially becoming the most famous metaverse company and raising global interest in the concept and its potential. Zuckerberg also announced that he would invest USD $50 million in partnerships with other firms to promote the metaverse concept and technology. Other leading tech companies like Google, Microsoft, and NVIDIA began investing in metaverse development and were joined by other kinds of companies like Nike, Walmart, Adidas, and PepsiCo.[3] But as with other technological revolutions and developments, the potential and promise are fraught with possible negative ethical and social consequences associated with the massive use of these technologies.

A white paper written by a team from *Telefónica* describes some of the social risks and challenging concerns associated with the metaverse. The authors acknowledge that the opportunities of the metaverse abound and add: "While we believe that the potential benefits will, by far, outweigh the risks, it is also important to reflect, in advance, on those potential risks, with the goal to mitigate them before they actually happen".[4] There are many potential risks and challenges that the metaverse raises, including technical, legal, security, business, tax, privacy, security, and users' well-being and safety (among many others). Some of the risks stem from deliberate malicious actions and others from unintended consequences of innocent ones. If the advancement of the metaverse or similar developments is inevitable, we agree with the team from *Telefónica* about the need to consider risks and abuses—especially regarding cyber-savvy terrorists, which others have also highlighted[5]—and think more carefully about them when moving forward. After briefly reviewing how terrorists have used online technologies over the last few decades, this special correspondence explores some potential uses of the metaverse by terrorists and suggests preemptive measures to minimise the risks of them doing so.

Online Terrorism

Terrorist networks have always relied on the mass media for publicity, psychological warfare, propaganda, and political achievements. The upsurge of media-focused terrorism has led several terrorism and communication scholars to reconceptualise modern terrorism within the framework of symbolic communication theory: "As a symbolic act, terrorism can be analysed much like other media of communication, consisting of four basic components: transmitter (the terrorist), intended recipient (target), message (bombing, ambush) and feedback (reaction of target audience)".[6] Dowling introduced the concept of "rhetoric genre," arguing that "terrorists engage in recurrent rhetorical forms that force the media to provide the access without which terrorism could not fulfil its objectives".[7] Weimann and Winn used the "theatre of terror" framing to analyse modern terrorism as an attempt to communicate messages by orchestrated violence.[8] The "theatre of terror" metaphor materialised dramatically in numerous events like the Munich Olympics attack in 1972 or the September 11, 2001, attacks in New York and Washington, DC. These media-oriented terrorist acts reached huge, frightened audiences in dramatic television broadcasts that turned them into media events.

Then came the World Wide Web and the Internet. At first, the Internet seemed to be a bridge between populations and cultures and an ideal promoter for interaction, businesses, education, communication, and politics. But with enormous growth in the size and use of the Internet, utopian visions of the promise of online media were confounded by the spread of incitement, pornography, violence, and the abuse of the Internet by extremist organisations. The online web of computer-mediated communication proved an ideal medium for extremists as communicators: it is decentralised, liberal, and open to all, cannot be subjected to genuine regulation or control, is not censored, and allows free access to everyone who wishes to partake in it. Groups committed to terrorising societies to achieve their goals have used the great virtues of the Internet—ease of access, lack of regulation, vast potential audiences, fast flow of information, and more—to their advantage.

As several studies have revealed, terrorists have used the Internet for a broad range of purposes,[9] a range far too broad to address comprehensively in this space. Researchers have illustrated many common patterns, such as how they use websites and social media to launch psychological campaigns, recruit and direct volunteers, raise funds, incite violence, and provide training. They also use it to plan, network, and coordinate attacks. Hoffman and Ware concluded that "today's far-right extremists, like predecessors from previous generations, are employing cutting-edge technologies for terrorist purposes."[10] As a general summary, it is widely agreed that cyber-savvy terrorists have been highly resourceful in adapting and using online platforms and have taken advantage of every new development, platform, and application for communicative and instrumental purposes. They began in the late 1990s with websites, forums, and chatrooms. Since 2014, they have been using the new social media (e.g. Facebook, YouTube, Twitter, and Instagram), eventually adding online messenger apps (e.g. WhatsApp and Telegram), new platforms (e.g. 4chan, 8chan, and TikTok), anonymous cloud storage, and the Dark Net. They have been quick to learn how to use the most recent advancements in cyberspace, and thus it is reasonable to assume that the metaverse is a new dimension that terrorists and violent extremists are poised to study, examine, and possibly utilise.

Metaverse As a Toolbox for Terrorism

Like all technological innovations, the metaverse introduces new prospects, threats, and challenges, including its potential use by terrorists and radical, violent extremists. Researchers at the National Counterterrorism Innovation, Technology and Education (NCITE) Centre in Omaha, Nebraska, concluded that "we see a potential dark side to the metaverse. Although it is still under construction, its evolution promises new ways for extremists to exert influence through fear, threat and coercion. Considering our research on malevolent creativity and innovation, there is potential for the metaverse to become a new domain for terrorist activity".[11] The metaverse may become a new territory for terrorist activity, a promising platform to improve and advance their online activities, including radicalisation, recruitment, training, fundraising and the coordination of attacks.[12] The two features that make the metaverse so attractive as a communication platform are presence and embodiment. Presence means that people feel they are communicating with one another directly, without any type of mediating channel or computer interface. Embodiment means that the users feel that their virtual body or avatar is their real, actual body. These two features of the metaverse enable a range of effective manipulation and deceptive influencing efforts.

According to the NCITE, the advancement of the metaverse will unlock new vulnerabilities that will be utilised by terrorists, complicating counter-terrorism measures in several ways. Thus, it additionally raises new challenges for counter-terrorism efforts, distinct from those already presented by social media platforms and earlier technologies, because of its considerably more immersive and emotional qualities based on its ability to produce parallel digital worlds.[13] It appears that like with other online new platforms, terrorists will want to add the metaverse to their present ecosystem, due to the operational benefits that it has over the present platforms. These benefits include substantial operational security, resilience to takedown, better interactivity, improved use of virtual contact, blending artificial intelligence with virtual reality,

and more. As noted earlier, it is vital to examine some of the potential uses of the metaverse by terrorists and suggest preemptive measures to minimise the potential risks. To assess potential threats, we began by scanning the literature on metaverse and similar platforms including published reports by international organisation like the European Commission, EUROPOL, the World Economic Forum, the Council of the European Union, academic papers, and conference reports. This scan resulted in a wide-ranging list of threats and risks that we then organised into eight categories, representing the most important and plausible challenges.

Indoctrination and Recruitment

Online recruitment and engagement are trademarks of modern extremism. The metaverse risks expanding this capability by making it easier for individuals to socialise and congregate.[14] Combining artificial intelligence with augmented reality within the metaverse will allow extremist leaders to convene and meet with their supporters, develop and sustain virtual idealistic societies, and increase their spheres of influence. Because of the extreme emotional environment made possible by the metaverse, it may be challenging for some individuals to differentiate between real life and virtual reality.[15] Some users may consider that what takes place in the metaverse is not factual even if it has real consequences for their lives. By blending artificial intelligence and augmented reality in the metaverse, online recruiters for terrorist or violent extremist groups will be able to meet in a virtual room with potential followers and entice them with visions of the future.

Similarly, a resurrected Osama bin Laden or Abu Bakr al-Baghdadi could interact with would-be supporters in a virtual garden or lecture hall inside the metaverse. The metaverse could help extremist leaders develop and maintain virtual idealistic and social communities, granting them power, enabling them to increase their ranks and spheres of influence with fewer challenges. Historical, spiritual, and idealistic subjects could be portrayed using avatars, bringing back to life dead terrorists and tyrannical leaders in a virtual resurgence, which could galvanise followers and inspire them to continue their struggles.[16]

The ability of the metaverse to impact users' emotions, as well as gather data on users' emotions could be abused by terrorists. Digital helmets and glasses will soon make it possible to capture individuals' feelings and responses in real time, allowing the exploitation of this information by terrorists and others. For instance, it will be possible to gather data on what individuals are glancing at within the metaverse, understand what is appealing to them, adjust the narrative accordingly, and then reach out to them. Terrorist groups could even produce their own metaverse, bringing together their supporters in a safe haven where diverse shapes of extremism are promulgated. This virtual world presents unique opportunities for extremists to remain in contact with each other and wield power over a radicalised community through events and regular gatherings. Extremist organisations could produce metaverse rooms where they freely distribute misinformation and hate speech, creating digital ecosystems for themselves that would be more technically advanced than the echo chambers and influence silos that are already prevalent on today's social media platforms. Thus, the metaverse could boost terrorist recruitment with new and appealing propaganda techniques in an online environment where emotional engagement is more robust, gradually obviating the need for offline meetings.

Already companies are using the metaverse to employ new staff; terrorist groups could do the same to recruit new members. In the future, numerous metaverse renditions or metaverse-like surroundings could materialise (depending on investments and the technological innovations created by companies like Meta), allowing the creation of regional metaverses connected to a state, company, or community. In this way, the physical territory lost by ISIS could be replaced by a virtual caliphate.

Planning and Coordinating Attacks

The metaverse presents new opportunities for planning, coordinating, preparing, and conducting acts of terror. Advanced planning and coordinating attacks can be achieved by surveillance and data collection, and extremist leaders could devise virtual backgrounds with models of any material structure, enabling them to move members through pathways leading to critical goals.[17] Members can learn feasible and efficient routes, coordinate alternative pathways if some are obstructed, and devise contingency strategies for cases of emergency. Augmented reality items, with virtual indicators such as arrows, can guide violent extremists, pinpointing marked targets when conducting an attack in the physical world. Operatives, potential attackers, and followers can plan from within their homes while also making social contacts and building trust in their counterparts, all the while presenting themselves to others in their chosen digital avatar design:

> *A resurrected bin Laden could meet with would-be followers in a virtual rose garden or lecture hall. Violent extremists can plot from their living rooms, basements, or backyards—all while building social connections and trust in their peers… When extremist leaders give orders for action in the physical world, these groups are likely to be more prepared than today's extremist groups because of their time in the metaverse.*[18]

The metaverse can be used to circumvent classical communication channels when designing and preparing attacks, as noted also by the Council of the European Union report.[19] Using the capabilities of the metaverse, terrorists can organise gatherings and share thrilling immersive experiences of attacks on various targets, reinforced by an outpour of images and videos of individuals' grievances. They could produce their own gaming space, for example, an Assassin's Creed–style game for jihadists. Likewise, emotional historical events could be recreated to shock and disturb users, galvanising followers. For example, significant terrorist attacks like the collapse of the World Trade Centre in New York or the attack at the Bataclan music venue in Paris could be reenacted in virtual reality.

Virtual Training

Terrorists have used various online platforms to teach and train attackers. The Internet is home to dozens of sites that provide information on how to build chemical and explosive weapons, how to launch attacks on infrastructure facilities, and how to conduct cyberattacks on computer systems. The metaverse could deliver a secure and more effective training and simulation climate for online instruction. Some companies already use the metaverse to provide combat

training to their employees. The emotional and immersive element of the metaverse makes training more lifelike and absorbing, transcending the experiences acquired with video games. At the same time, VR technology makes the metaverse vulnerable to mishandling by violent extremists and terrorists, who could use it to provide and obtain combat training, including training in precision shooting, tactical training, hostage taking, and surveillance. Finally, the gaming sector of the metaverse is far more susceptible to bolstering extremist activity and radicalisation because of the absence of oversight, the preservation of anonymity, and the ability to supply combat training.[20]

New Targets

The latest virtual and mixed-reality environments have the potential to create new targets, such as structures, events, and individuals in the physical and virtual worlds.[21] Terrorists can discover virtual targets in the metaverse such as economic and social events. For example, a 9/11 commemorative service produced and hosted within the virtual domain could become a target for violent extremists who would re-enact the attack. Likewise, a metaverse wedding could be interrupted by attackers who object to the religious or gendered pairing of the partners, and similarly, a symbolic killing of avatars by terrorists in various gruesome ways. These actions would take a psychological toll on the users and result in real-world suffering. Similarly, damaging an augmented or virtual reality business can result in real-world financial losses.[22] Like physical locations, new virtual and mixed reality spaces may become the potential new targets. As technology evolves and becomes smaller and better incorporated into individuals' day-to-day lives, it may become increasingly difficult to switch off the metaverse or disregard the damage it could cause.

Spreading Disinformation

Disinformation has acquired a dual meaning: on one hand, as fabricated or fake news, which circulates online and offline, and on the other, as a powerful weapon used to discredit authorities, institutions, and media channels. We focus first on the former interpretation. The current Web 2.0 has given rise to the spread of fake news, disinformation, and lies because of the absence of effective gatekeeping and fact-checking, especially on social media outlets. Terrorists and extremists soon realised the potential of online channels for the spread of disinformation that may serve to fuel debate, distrust, loss of confidence, and panic. Because this may destabilise society and communities, law enforcement has been tasked to protect against such malicious activities, but the challenges that disinformation poses in the metaverse are even more troublesome. Rand Waltzman, an information scientist at the Rand Corporation, wrote about metaverse and disinformation.[23] Based on 40 years of experience as a programme manager at the Defense Advanced Research Projects Agency (DARPA), Waltzman warned that we are not even close to being able to defend users against the threats posed by the metaverse, where malicious actors will be able to take the age-old dark arts of deception and influence to new heights or depths:

> *At the heart of all deception is emotional manipulation. Virtual reality environments, such as Facebook's (now Meta's) metaverse, will enable psychological and emotional manipulation of its users at a level unimaginable in today's media... The metaverse will usher in a new age of mass customization of influence and manipulation. It will provide a powerful set of tools to manipulate us effectively and efficiently. Even more remarkable will be the ability to combine tailored individual and mass manipulation in a way that has never before been possible.*[24]

The two special communicative features of the metaverse, namely presence and embodiment, are very relevant for effective spread of disinformation, manipulation, and deceptive influencing.

Desensitisation

Since the 1990s, concerned educators, parents, politicians, and researchers have railed against violent video games, their primary concern being that certain games desensitise players to extreme violence. Although there have been a small number of instances when experience with violent video games was linked to criminal acts by young people (most notably, tragic school shootings), scholarly research has largely refuted a causal connection.[25] However, studies have highlighted desensitisation to violence as a risk factor: playing violent video games was correlated with lower empathy, desensitisation to violence at both the neural and behavioural levels, and decline of cognitive and emotive reactions to violent impulses.[26] The absence of compassion and desensitisation may be encouraged by in-game ethical disengagement methods that selectively halt ethical management tools, contributing to the endorsement and practice of violence to a more significant extent.[27] The risk of desensitisation is heightened in the metaverse. While exploring some popular metaverse platforms, journalist Yinka Bokinni had a harrowing realisation:

> *The worst thing is how numb you become. The casual way people were using extremely violent language that was homophobic, racist and sexist meant that after my third or fourth dive into the metaverse, I became desensitized to it... It's a space in which it's become normalized.*[28]

Similar concerns were raised by Kieron Allen who argued that the metaverse, through user immersion, may have an alarming desensitising effect.[29] The most obvious mechanism by which metaverse games can facilitate radicalisation processes is that of the popular first-person shooter games, which can desensitise the user to violence and cause moral disengagement.[30] When analysing a virtual world called *Second Life* from the extremist viewpoint, Cole discovered that using an avatar exposed to the explicit content of radical Islamic propaganda, "continuous auditory and visual stimuli can cause a person to self-identify with an extremist group's views".[31] Bajwa concluded a study on "Malevolent Creativity & the Metaverse" with the statement: "Results show that the concatenation of malevolent creativity, innovation and subcultural extremism may bridge the gap between ideation of mass shootings and mobilization".[32]

Financing Terrorism

With the increasing use of cryptocurrencies, the metaverse offers terrorists greater prospects of anonymous funding.[33] The financial blacklists—and more commonly, the steps used at present to counter the financing of terrorism—would have little effectiveness in the metaverse. Blockchain technology and cryptocurrencies are the foundation blocks of the metaverse, enabling users to supply digital identification and verification of ownership, digital display of acquisitions such as non-fungible tokens (NFTs), and crypto value transfer. Individuals will presumably be requested to possess a cryptocurrency wallet to access the metaverse and maintain their digital investments, stimulating an upsurge in their use. There are growing concerns about the utilisation of cryptocurrencies in terrorist financing because of anonymity, the potential of making immediate payments, and the capability to conduct cross-border transfers without any oversight by any government authority or bank. For example, crypto assets could be used for money laundering or fundraising. Tracing interactions will be far more difficult in the metaverse because of its strong ties with cryptocurrencies. One can envision money being made dealing with identity artifacts, such as swastikas or terrorist symbols, as NFTs, which are then used to customise avatars and portray one's affiliation with terrorist organisations. Terrorist groups can boost their financial reserves and bolster their communities through online shows or avatar contests, which are presently being organised to increase funds for violent right-wing extremism. Such decentralised financing could assist terrorist organisations in devising their online ecosystems and managing their metaverses, a concern noted in the report of the Council of the European Union.[34]

Financial Terrorism

Terrorists have used various forms of cybercrimes to raise funds, launder money, steal money, and attack financial institutions. The metaverse may expand their financial arsenal. According to a report by Elliptic, USD $14 billion worth of crypto assets has been declared stolen owing to scams in 2021 alone.[35] The more common dangers are the diverse types of phishing and fraud scams that transpire within the metaverse, entangling malicious fake sites devised to obtain their targets' crypto assets. Those sites can impersonate the login panel of a prominent metaverse platform such as Decentraland, a global network of users in the metaverse, using meta-related coins for cryptocurrency exchange. One of the successful strategies used by cybercriminals and cyberterrorists is social engineering, which manipulates individuals' psychological vulnerabilities and has become a significant threat within the metaverse. There are many methods that scammers use to earn individuals' trust. They can act to represent authorised metaverse projects by acquiring control of notable social media accounts, imitating trusted organisations or avatars within the metaverse, and conning individuals to click on a phishing link or transmit funds to the scammers' wallets. Similarly, scammers can act as technical staff for metaverses and mislead users into transferring private keys or leading them to a phony site by pretending they want to assist them with a technical problem.

A prominent fraud threat for crypto investors is the "rug pull," when the developers of a cryptocurrency project desert the project abruptly, seizing users' funds with them. Usually, when launching a metaverse project, developers detail their objectives in a roadmap, whether

it is online game development or charity fundraising, after which they begin campaigns to collect funds to carry the project to the subsequent stage. These techniques may be useful for terrorists and extremists who already use online platforms for fundraising and fake charity activities.[36]

Can We Have a Safer Metaverse?

The metaverse is still in the developmental stage, incorporating real and virtual realities, using artificial intelligence, virtual reality, and other augmented reality software to create a new virtual platform. It is not easy to assess the impact of this future online platform though several studies on the effects of virtual reality outlets (for example in the context of gaming, teaching, training, and more) did provide empirical evidence on the impact on users mainly in terms of involvement, emotional impact, immersion, and excitement. But can we limit the use of this future platform or similar developments by terrorists and extremists? Will it have adequate safeguards built into it to protect its functions and uses from being abused?

For some time, a game of cat and mouse has been played between state actors and online terrorists. This has been changing since important non-state actors, like META, have been assuming a bigger role in the war against terrorism. The old battlefield has changed into one that is no longer just physical but also virtual, where non-state actors play a key role, given their influence and expertise.[37] As both sides are trying to outmanoeuvre each other, a vicious cycle of innovations and countermeasures takes shape. It is necessary to break this cycle with a new long-term strategy, with preemptive measures requiring the participation of all relevant partners. Several steps are needed to devise a concrete and interconnected strategy that will thwart terrorist organisations before they strike first.

Public and Private Partnership (PPP)

Most of the online infrastructure, including communication systems and platforms, is privately owned, but it is largely in the hands of state authorities to act upon its security. This creates a situation in which market forces alone are not sufficient to provide security in most of the critical online sectors. At the same time, the state is incapable of providing full security on its own. Therefore, cooperation between the state and the private sector in cyber protection is not only useful but inevitable. Public-private partnerships (PPP), a form of cooperation between the state and the private sector, are widely seen as necessary to combat terrorist use of the Internet in general and cyberterrorism in particular.[38] The fundamental character of PPP can be described as follows: "Its goal is to exploit synergies in the joint innovative use of resources and in the application of management knowledge, with optimal attainment of the goals of all parties involved, where these goals could not be attained to the same extent without the other parties".[39] According to Antigone Davis, the Global Head of Safety at Meta, to provide wide-ranging security as the metaverse develops, it is critical to partner with other actors within governments, industries, academia, and civil society.[40] Joint, coordinated contributions to the metaverse are a sensible approach that will require research, partnership, and investment in security. For example, as Davis noted, Meta is investing in controls that permit users to

administer and report troublesome content and conduct security tooling design to create immersive experiences. Yet Meta, or any other company, cannot do this alone but needs allies from all segments of society to create a safer and more interconnected network.

Early Engagement

During the early phases of the development of any product, the foundations are laid based on prerequisites established by the developers. Thus, redesigning a system to satisfy certain requirements is far more challenging than incorporating these requirements from the start. For example, it is vital for civil society and law enforcement to convey their demands early during the adoption of the metaverse by engaging with the main actors designing metaverse platforms. This allows both sides to understand how to make the metaverse more secure, adjust lawmaking, and prepare for law enforcement.[41] It would be informative to discover how individuals intend to contact the moderators of a platform or the police. If this means that there should be a way to reach the appropriate authority directly, such a component should be considered. There should be an API standard that law enforcement could use to connect to all relevant platforms for policing purposes. Such requests should become part of an industry criterion for the interoperability of future metaverses, like the present Metaverse Standards.[42] Metaverse and similar platforms will also operate in various regulatory landscapes. Given the legislation in Western societies, it seems likely that some laws (and maybe new ones) will limit the exploitation of the metaverse and cause the providers to act and implement safeguards.

Monitoring the Metaverse

When new technologies emerge, they are largely ignored by security and law enforcement as initially was the Internet. The Europol report on the risks of the metaverse noted that "[l]egislating for new technology is often compared to driving a car only using the rearview mirror. It is often done in retrospect, and by that time new dangers are ahead of you, it is too late".[43] Yet, societies, governments, and security agencies learned to use cyber surveillance and cyber monitoring methods to fight crime, terrorism, and online abuse. Governments such as Estonia, Denmark, Norway, and Sweden have been supporting online police monitoring. Such state support is crucial to producing invaluable experience within virtual reality. When police officers are active online, they are more accessible to individuals living in secluded areas and to individuals who spend much of their time online. Because of the large variety of open online platforms, gaining experience on designated primary platforms is essential. And because online platforms are naturally global, constructing a network of law enforcement specialists can be most beneficial. The EUROPOL report concluded that "[w]e recommend law enforcement to monitor the development of the metaverse and to start building experience with online policing and early iterations of the metaverse. Doing this officially will help organisations stay informed on the subject and enable them to assess developments accurately, answering threats as they emerge."[44] However, monitoring online platforms raises the ethical issues of privacy, free speech, and civil liberties. Thus, monitoring the metaverse and identifying users should follow the ideal balance between protecting national security and minimising the unintended consequences to human rights, as outlined in several publications.[45]

Identification Policy

At present, it is quite easy for cyber-savvy individuals to commit unethical or illegal activities online and evade consequences because the appropriate authorities cannot identify them. If individuals enter the metaverse through a virtual private network (VPN), identifying them when they break the rules or perpetrate a crime becomes more difficult.[46] There should be a method by which individuals' identities can be confirmed before being permitted to enter the metaverse. The joke about Web 1.0 was that "no one knows you are a dog." Web 2.0 tried to solve the identity problem by authenticating users, starting with Facebook's "real name" policy. Creating a mainstream metaverse should require an equally strong identification policy, resulting in solid motivations for metaverse communities to protect themselves. Requiring individuals to identify themselves when creating their accounts and avatars may reduce identity theft on a large scale. Users could also be requested to confirm their ages to stop children from entering dangerous areas within the metaverse.[47]

User Education

Criminals and terrorists are highly creative and manage to keep a step ahead of regulators and businesses in their measures to safeguard data. Educating users on measures they can take to safeguard their identities and acquisitions within the metaverse and the preventive actions they can take will play an important role. The European Commission's revised digital education action plan seeks to ensure that 70 percent of 16–74-year-olds in the EU have at least a fundamental digital understanding by 2025.[48] Unfortunately, many adults have been reluctant to spend time or money gaining cybersecurity proficiency, making them ripe targets for cyberattacks. In contrast, because young people are often keen to learn, schools will be especially important for providing adequate training on cybersecurity.[49] The knowledge gained by these students can assist them in providing a cyber defence for themselves and others.[50] Cybersecurity education has also been shown to change students' perspectives, and cybersecurity awareness can help young Internet users profit from the Internet without becoming targets of cyberattacks.[51] Delivering essential knowledge to improve metaverse users' understanding of cybersecurity is vital for reducing the risks of the platform. This requires a broader education in the online world and how it operates. Moreover, such defensive education should not be limited to school-age populations: firms and companies, as well as advanced educational systems like colleges and universities, may be involved in such digital education.

Confronting Financial Crime within the Metaverse

Combatting financial crime within the metaverse requires a multi-level approach involving many stakeholders operating jointly. This is certainly a challenge when considering the potential use of the metaverse by terrorists and extremists. A special report on "Financial Crime in the Metaverse is Real: How Can We Fight Back?" prepared by the European law firm of *Wolf Theiss,* describes the particulars of such multi-level counter-operation.[52] End users must be mindful that partaking in any new technology makes them possible targets of criminal actors including terrorists. Therefore, to guard against suspicious incursions and fraud scams, individuals must remind themselves to think logically and not allow their fear of missing out to lead to impulsive

decisions. Furthermore, companies operating inside the metaverse must cooperate with safety and risk teams early to pinpoint potential vulnerabilities, warn their employees about these threats, and test apps rigorously before they go live. To safeguard against code exploits, users and companies must participate in metaverse projects where smart contract codes are designed and examined by a technically trustworthy and respected team. Finally, considerable measures have been taken by states and governments to devise practical legal measures to control and combat crimes linked to crypto assets. To meet this challenge, the EU has been involved in giving directives to align its collective membership legal frameworks, for instance, the 5th AML Directive (EU) 2018/843 and the Directive (EU) 2019/713.

Conclusion

When Zuckerberg announced Meta, in October 2021, he also announced that privacy and security should be built into the metaverse from day one. There are serious doubts about the success of the metaverse. Currently, AI hype, especially around large language models (LLMs), has overtaken metaverse-related hype in the mass media and in academic discourse. This may lead to reductions in investments and developments of metaverse and metaverse-adjacent activity. But even the most pessimistic speculations about the future of the metaverse do not rule out the emergence of fused platforms, merging the physical and virtual realities using advanced communication platforms. It is not yet clear how these developments will turn out, but the technology is advancing apace, promoted by numerous global technology giants.

The history of the Internet and related technologies has taught us that multiple unanticipated effects are likely to arise, so unexpected side effects of innovation may have most significant consequences. Whatever the outcome may be, all relevant parties must partake in the development of metaverse or similar platforms and keep up to date on its future products. Understanding what is being devised by potential abusers will be essential for developing a preemptive strike strategy to counter terrorist attacks within the metaverse. There is an opportunity to proactively prepare and contribute to shaping a safer metaverse and similar platforms. There are already numerous tools and initiatives deployed in online platforms that could be retooled for deployment in the metaverse. This includes initiatives from public-private partnerships such as the EU Internet Forum (EUIF) to tech company initiatives, such as GIFCT, from legislation such as the EU's Terrorism Content Online Regulation (TCO) to the UN-supported Tech Against Terrorism.

Gabriel Weimann is a professor at Reichman University (Israel), a professor (emeritus) at the University of Haifa (Israel), and visiting professor at Georgetown University (Washington, DC). Over the course of his long career, he has carried out research on a range of topics, including political communication, online terrorism, extremism, and cyberterrorism. He has published nine books and more than 200 scientific works, and won numerous research grants and scholarly awards.

Roy Dimant is a graduate student at Reichman University and a research intern at the International Center for Counter-Terrorism (ICT) at Reichmann University.

Endnotes

1 Neal Stephenson, *Snow Crash* (New York Bantam Book, 1992).

2 Mark Zuckerberg, "Founder's Letter 2021", Meta Website (October 28, 2021), https://about.fb.com/news/2021/10/founders-letter/.

3 Aaron Drapkin, "Metaverse Companies: Who's Involved and Who's Investing in 2022", *TechCo* (October 25, 2022), https://tech.co/news/metaverse-companies-whos-involved-whos-investing.

4 Richard Benjamins, Rubio Yaiza, and Chema Alonso, "Social and Ethical Challenges of the Metaverse", Special Report by *Telefónica* (May 2022), https://www.telefonica.com/en/wp-content/uploads/sites/5/2022/05/Social-and-ethical-challenges-metaverse-EN.pdf,.

5 Zefeng Chen, Jiayang Wu, Wensheng Gan, Zhenlian Qi, "Metaverse Security and Privacy: An Overview", arXiv (2022) https://arxiv.org/abs/2211.14948; Joel Elson, Austin Doctor, and Sam Hunter, "The metaverse offers a future full of potential – for terrorists and extremists", *The Conversation* (January 7, 2022), https://theconversation.com/the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too-173622; Delphine Debuire, "Terrorist use of the Metaverse: new opportunities and new challenges", *The Security Distillery* (April 12, 2022), https://thesecuritydistillery.org/all-articles/terrorism-and-the-metaverse-new-opportunities-and-new-challenges.

6 Phillip Karber, "Urban Terrorism: Baseline Data and a Conceptual Framework." *Social Science Quarterly* 52, 527–33, (1977), 33.

7 Ralph Dowling, "Terrorism and the Media: A Rhetorical Genre", *Journal of Communication* 56, (1986):12–24.

8 Gabriel Weimann and Conrad Winn, *The Theatre of Terror: Mass Media and International Terrorism* (New York: Longman, 1984).

9 Gabriel Weimann, *Terror on the Internet: The New Arena, The New Challenges* (Washington, DC: United States Institute of Peace Press, 2006); Gabriel Weimann, *Terror in Cyberspace: The Next Generation* (New York: Columbia University Press, 2016); and Aaron Zelin, *The State of Global Jihad Online* (Washington, DC: New America Foundation, 2013).

10 Bruce Hoffman, and Jacob Ware, "Are We Entering a New Era of Far-Right Terrorism?" *War on the Rocks,* (November 27, 2019), https://warontherocks.com/2019/11/are-we-entering-a-new-era-of-far-right-terrorism/.

11 Elson et al., "The metaverse offers a future full of potential – for terrorists and extremists", 3.

12 Debuire, "Terrorist use of the Metaverse: New opportunities and new challenges".

13 Council of the European Union, "The Metaverse in the Context of the Fight Against Terrorism", Special Report (June 2, 2022), https://data.consilium.europa.eu/doc/document/ST-9292-2022-INIT/en/pdf.

14 Elson et al., "The metaverse offers a future full of potential – for terrorists and extremists".

15 Council of the European Union, "The Metaverse in the Context of the Fight Against Terrorism".

16 Ibid.

17 Elson et al., "The metaverse offers a future full of potential – for terrorists and extremists".

18 Ibid., 5.

19 Council of the European Union, The Metaverse in the context of the fight against terrorism.

20 Sara Senno, "The Metaverse, an opportunity for society or terrorism?", AMISTADES report (April 22, 2022), https://en.amistades.info/post/metaverse-an-opportunity-for-society-or-terrorism.

21 Elson et al., "The metaverse offers a future full of potential – for terrorists and extremists".

22 Ibid.

23 Rand Waltzman, "Facebook Misinformation Is Bad Enough. The Metaverse Will Be Worse", *The Washington Post* (August 22, 2022), https://www.washingtonpost.com/opinions/2022/08/22/metaverse-political-misinformation-virtual-reality/.

24 Ibid., 1.

25 Patrick M. Markey, Charlotte N. Markey, and Juliana E. French, "Violent Video Games and Real-World Violence: Rhetoric versus Data", *Psychology of Popular Media Culture* 4 (2015), pp. 277–295, http://dx.doi.org/10.1037/ppm0000030; Tom Grimes and Lori Bergen, "The Epistemological Argument Against a Causal Relationship Between Media Violence and Sociopathic Behavior Among Psychologically Well Viewers". *American Behavioral Scientist* 51, no. 8 (2008), pp. 1137–1154, https://doi.org/10.1177/0002764207312008; Scott Cunningham, Benjamin Engelstätter and Michael R. Ward, "Violent Video Games and Violent Crime", *Southern Economic Journal* 82

(2016), pp. 1247–1265, http://dx.doi.org/10.1002/soej.12139; Patrick M. Markey, James D. Ivory, Erica B. Slotter, Mary Beth Oliver and Omar Maglalang, "He Does Not Look Like Video Games Made Him Do It: Racial Stereotypes and School Shootings", *Psychology of Popular Media* 9, no. 4 (2020), pp. 493–498, https://doi.org/10.1037/ppm0000255.

26 Jeanne F. Brockmeyer, "Desensitization and Violent Video Games: Mechanisms and Evidence", *Child and Adolescent Psychiatric Clinics of North America* 31, no. 1 (January 2022), pp. 121–132, https://doi.org/10.1016/j.chc.2021.06.005; Ewa Miedzobrodzka, Johanna C. van Hooff, Elly A. Konijn, and Lydia Krabbendam, "Is it Painful? Playing violent video games affects brain responses to painful pictures: An event-related potential study", *Psychology of Popular Media* 11, no. 1 (2022), pp. 13–23. https://doi.org/10.1037/ppm0000290.

27 Albert Bandura, "Selective Activation and Disengagement of Moral Control", *Journal of Social Issues* 46, no. 1 (1990): 27–46, https://spssi.onlinelibrary.wiley.com/doi/10.1111/j.1540-4560.1990.tb00270.x; Tilo Hartmann, Maja Krakowiak, and Mina Tsay-Vogel. "How Violent Video Games Communicate Violence: A Literature Review and Content Analysis of Moral Disengagement Factors". *Communication monographs* 81, no. 3 (2014): 310–332. https://www.tandfonline.com/doi/abs/10.1080/03637751.2014.922206.

28 Yinka Bokinni, "A barrage of assault, racism and rape jokes: my nightmare trip into the metaverse", *The Guardian* (April 25, 2022), https://www.theguardian.com/tv-and-radio/2022/apr/25/a-barrage-of-assault-racism-and-jokes-my-nightmare-trip-into-the-metaverse.

29 Kieron Allen, "How Desensitization Through Immersion Could Have Real-World Consequences", *Acceleration Economy* (April 22, 2022), https://accelerationeconomy.com/metaverse/how-desensitization-through-immersion-could-have-real-world-consequences/.

30 Linda Schlegel, "How Video Games Could Facilitate Radicalization Processes", Regional Cooperation Council report (April 13, 2020), https://www.rcc.int/swp/news/278/how-video-games-could-facilitateradicalization-processes.

31 James Cole, "Radicalisation in Virtual Worlds: Second Life through the Eyes of an Avatar". *Journal of Policing, Intelligence, and Counter Terrorism*, 7, no. 1 (2012): 66–79. http://dx.doi.org/10.1080/18335330.2012.653197, 38.

32 Aman Bajwa, "Malevolent Creativity & the Metaverse: How the immersive properties of the metaverse may facilitate the spread of a mass shooter's culture", *The Journal of Intelligence, Conflict, and Warfare* 5, no. 2 (2022): 32–52, https://journals.lib.sfu.ca/index.php/jicw/article/view/5038, 32.

33 Debuire, "Terrorist Use of the Metaverse: New opportunities and new challenges".

34 Council of the European Union, The Metaverse in the context of the fight against terrorism.

35 WolfTheiss, "Financial Crime in the Metaverse Is Real: How Can We Fight Back?", *WolfTheiss report* (October 3, 2022), https://www.wolftheiss.com/insights/financial-crime-in-the-metaverse-is-real/.

36 Weimann, *Terror on the Internet* (2006); *Terror in Cyberspace: The Next Generation* (2016).

37 Beatrice Peterson, "Meta says it will share software in attempt to combat terrorism, human trafficking", *ABC News* (December 13, 2022), https://abcnews.go.com/Technology/meta-share-software-attempt-combat-terrorism-human-trafficking/story?id=94882414.

38 Weimann, *Terror in Cyberspace: The Next Generation* (2016).

39 Myriam Dunn Cavelty, "Public–Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection", *International Journal of Critical Infrastructure Protection* 2, no. 4 (2009): 179–187, http://www.academia.edu/462519/Public-Private_Partnerships_Are_No_Silver_Bullet_an_Expanded_Governance_Model_for_Critical_Infrastructure_Protection, 179.

40 World Economic Forum, "How to Address Digital Safety in the Metaverse", (January 14, 2022), https://www.weforum.org/agenda/2022/01/metaverse-risks-challenges-digital-safety/.

41 EUROPOL, "Policing in the Metaverse: What Law Enforcement Needs to Know", an Observatory Report from the Europol Innovation Lab (2022), https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf.

42 Metaverse Standards Forum, "Leading Standards Organizations and Companies Unite to Drive Open Metaverse Interoperability", (October 24, 2022), https://metaverse-standards.org/news/press-releases/leading-standards-organizations-and-companies-unite-to-drive-open-metaverse-interoperability/.

43 EUROPOL, "Policing in the Metaverse: What Law Enforcement Needs to Know", 6.

44 Ibid., 26.

45 Weimann, *Terror in Cyberspace: The Next Generation*, 221–254.

46 Katie Rees, "5 Vital Safety Features the Metaverse Needs", MUO online (February 28, 2022), https://www.makeuseof.com/metaverse-safety-features/.

47 Car Polona, André, Madiega and Maria, Niestadt, "Metaverse: Opportunities, Risks and Policy Implications", *Policy Commons* (June 24, 2022), https://policycommons.net/artifacts/2476871/metaverse/3498933/.

48 European Commission, *Digital Education Action Plan 2021-2027* (2020), https://education.ec.europa.eu/focus-topics/digital-education/action-plan.

49 Eric Amankwa, "Relevance of Cybersecurity Education at Pedagogy Levels in Schools", *Journal of Information Security* 12 no. 4(2021): 233–249, https://www.scirp.org/journal/paperinformation.aspx?paperid=111804; Nurul Amirah Abdul Rahman, Izza Hanis Sairi, Nurul Akma Zizi, and Fariza Khalid, "The importance of cybersecurity education in school". *International Journal of Information and Education Technology* 10, no. 5 (2020): 378–381, http://www.ijiet.org/vol10/1393-JR419.pdf.

50 Amankwa, "Relevance of Cybersecurity Education at Pedagogy Levels in Schools".

51 WolfTheiss, "Financial Crime in the Metaverse Is Real: How Can We Fight Back?"

52 Ibid.

About

Perspectives on Terrorism

Established in 2007, *Perspectives on Terrorism* (PT) is a quarterly, peer-reviewed, and open-access academic journal. PT is a publication of the International Centre for Counter-Terrorism (ICCT), in partnership with the Institute of Security and Global Affairs (ISGA) at Leiden University, and the Handa Centre for the Study of Terrorism and Political Violence (CSTPV) at the University of St Andrews.

Copyright and Licensing

Contact

E: pt.editor@icct.nl
W: pt.icct.nl

Universiteit Leiden

HANDA CSTPV