6-2024

The Metaverse as a Future Threat Landscape: An Interdisciplinary Perspective

Sam T. Hunter

Alexis L. d'Amato

Joel Elson

Austin C. Doctor

Averie E. Linnell

PT PERSPECTIVES ON TERRORISM

RESEARCH ARTICLE

The Metaverse as a Future Threat Landscape: An Interdisciplinary Perspective

Sam Hunter,* Alexis L. d'Amato, Joel S. Elson, Austin C. Doctor, and Averie Linnell

Volume XVIII, Issue 2
June 2024

ISSN: 2334-3745
DOI: 10.19165/2024.2598

Abstract: In response to the emergence of new, paradigm-shifting technology that increases capability for the benefit and – as is the focus of this work – harm, we sought to provide contributions across three key areas. First, as a foundation, we provide a definition of the ambiguous and, at times, confusing term 'metaverse' and outline its unique characteristics as an emerging ecosystem. Second, we synthesise definitional framing with the violent extremist literature to offer guidance on how the metaverse can (and currently is), manifest in terrorist and extremist activities, such as recruitment, planning, finance, and malevolent creativity. We offer that while the use of the internet is not a novel application for such activities and groups, the metaverse and related technologies afford new opportunities for how the internet is used to advance violent missions and objectives. Third, we draw on psychology literature to offer potential mechanisms by which the metaverse may emerge as a future threat landscape. Future areas of research are also discussed.

Keywords: Metaverse, technology, future threats, novel threats, violent extremism, terrorism, psychology, mixed reality

* *Corresponding author: Sam Hunter, University of Nebraska, email: samuelhunter@unomaha.edu*

Introduction

In 2022, three teens plotted to destroy a virtual Russian building (formerly the KGB building, now the Federal Security Service or FSB building) in the popular *Minecraft* gaming platform.[1] Investigators also reportedly found evidence of testing explosive devices that could have been used in a physical attack that, although unlikely to be successful, would have at least partially mirrored the virtual destruction. All three teens were tried in the Russian court system, with one 15-year-old sentenced to five years in prison after failing a lengthy appeal process.[2] A 2022 report from the *Wall Street Journal* outlined the use of non-fungible tokens (NFTs) by an alleged member of Islamic State in Iraq and Syria (ISIS) to both spread extremist propaganda, as well as assess capability around acquiring financial support for the terrorist organisation.[3] Most recently, members of the Houthi, an Iranian-linked terrorist organisation based in Yemen, posted several videos of a hijacking of a cargo ship in the Red Sea. Close inspection of the videos reveals the use of 360-degree video capture devices, allowing groups, such as the Houthi, to share their footage in an immersive, virtual reality format. More directly, this event illustrates how terror groups can not only share videos as part of their propaganda arm but are now afforded the opportunity to allow potential recruits to virtually "go along for the ride" as well. As we will discuss later, this virtual experience can become nearly indistinguishable, from a neuroscience perspective, from having actually experienced the event itself.[4]

The emergence of blended physical and digital environments, known more colloquially as the *metaverse,* has resulted in notable opportunities for collaboration and engagement. Outlined above and discussed in some detail by others, there is a darker side of this emerging landscape and, with it, the potential for use by malign actors, including terrorists and violent extremists.[5] In light of the rapid growth of this emerging technology and associated ecosystem and potential for malign use, we set out to accomplish three goals in the present effort. First, we aim to provide clarity around the ambiguous language used when describing the metaverse and associated technologies. Second, we discuss how the metaverse as an ecosystem provides opportunities for exploitation by malign actors. Finally, we seek to provide guidance as to how and why the metaverse represents a unique and potentially impactful tool for terrorist actors. Specifically, we utilise existing literature from the fields of psychology and computer science to provide guidance as to the mechanisms by which the use of metaverse technologies may be leveraged for harm. In doing so, we aim to go beyond simply describing the problem and providing insight into how and why such technologies represent a new frontier of threat, thereby permitting greater clarity around future interventions and mitigation approaches.

Defining the Metaverse

As with many emerging terms and new forms of technology, (e.g., artificial intelligence, blockchain, and even the internet), the metaverse has been many different things to many different individuals. Although the term *metaverse* first appeared in the 1992 novel Snow Crash, exponential innovation has led to many technological capabilities that were unimaginable, even in science fiction writing of that era. The term metaverse continues to evolve as technology, application, and social views shift and change over time. This change in meaning has been an understandable source of some consternation for some (e.g., Apple's refusal to use the term metaverse, opting instead for the term *spatial computing*). While some continue to think of the metaverse as a purely digital world, industry and academics are increasingly moving beyond this framing, recognising the future implications of technologies that allow for the manipulation of digital information within physical and digital space.

As technology progresses, inevitable change will be experienced in terms of the users, environments, interactions, resources, and systems that are tied together because of the

interconnectedness between the digital and physical. For our discussion here, we follow emerging consensus and define the metaverse as the ecosystem surrounding the blending of physical and digital realities.

The metaverse is defined here as an ecosystem, which includes a combination of various elements that enable humans to experience it directly or indirectly. The term *ecosystem* has been employed to describe the interconnected elements and stakeholders in domains such as information systems and terrorism.[6] Viewing the metaverse as an ecosystem provides a holistic perspective, emphasising both the individual components and their interconnectedness, while fully embracing the potential for growth and change. As an ecosystem, it consists of physical infrastructure, platforms, applications, digital goods, artefacts, human users, communities, standards, and governance. Humans can engage with the metaverse through human-computer interfaces like head-mounted displays or traditional computing devices such as mobile phones. These interfaces offer different levels of interaction, from direct manipulation of computer-generated assets (e.g., spinning a virtual globe) to mediated interfaces affording indirect interaction (e.g., turning on a physical light switch to illuminate a virtual lamp). The metaverse can be observed and engaged with across a spectrum of mediums, ranging from predominantly physical to predominantly digital.[7] On the physical end of the spectrum, augmented reality (AR) devices overlay digital content on top of the physical environment. Conversely, virtual reality (VR) devices fully immerse users in a digital space. Mixed reality (MR) represents an intersection of these environments, where the physical and digital realities blend seamlessly. The term extended reality (XR) includes the entire continuum of technology. The metaverse encompasses this plus an entire ecosystem, including the social and economic dynamics surrounding the emergence of these technologies.

Although XR technologies are crucial for immersive digital experiences, it is necessary to provide additional guidance on the unique aspects of the metaverse. We offer that differentiating properties separating the metaverse from non-metaverse content are best represented by the concepts of spatiality, interoperability, and persistence (SIP). Formally, *spatiality* refers to the orienting of objects in relation to one another. As humans, our sensorial experience of reality is predominantly spatial, allowing users to move and interact with objects and others in a way that feels natural and intuitive. Spatial reasoning and embodied cognition suggest that the human mind is a product of evolutionary adaptations to challenges in a three-dimensional environment. Humans are capable of spatial reasoning and utilise several physical adaptations to allow better interaction in the natural environment and, by extension, spatial digital environments. The second feature, *interoperability*, describes the ability to exchange data and move between experiences, systems, and information technology components efficiently and seamlessly. Today, an object purchased in one virtual experience cannot readily be brought into another. For example, an intelligent robot assistant purchased in one virtual work environment cannot be brought into the digital office of a competing platform provider.

Digital apparel from a work environment cannot be worn in a recreational game by a different developer. Similarly, virtual experiences are often disconnected from one another and do not allow for a user to move between experiences in a seamless manner. Yet, as the metaverse evolves, this interoperability will be key for long-term functionality and sustainability. Finally, *persistence* refers to the ability of an object or data to remain stored and accessible over time. A lack of persistence is presently observed in many of today's video games. An object in a virtual reality game can be destroyed and then restored, or a structure built in a game vanishes when the player logs off. In the metaverse, virtual objects and assets can (and many will) persist over time, serving to establish real value, meaning, and connection. NFTs, for example, are unique digital assets that can be augmented in a way that enhances or detracts from their value.

Although metaverse applications may not always ensure complete persistence, they will be closely tied to an enduring experience. There may be, for example, situations where persistence is intentionally not preserved, such as an object or experience within that is dynamically generated or time-limited to achieve a purpose, such as increased rarity. From an extremism and terrorism perspective, this persistence means that many objects in the metaverse will have value due to their rarity and unique, persistent quality.

It is important to note that several other key aspects (scalability, immersion, etc.) of the metaverse are still crucial in shaping the overall vision and values of the metaverse, even if they are not strictly necessary for its *technical* functioning and sustainability. As an example, scalability is not an absolute requirement for the metaverse to operate as an ecosystem since there could be hypothetical situations where an experience is designed for a small group or even a single individual. Immersion is also critical (though not a wholly essential feature), as experience can exist where various levels of immersion are realised at different moments in time, and there is no minimum or maximum threshold that needs to be maintained. Rather, immersion is an experienced phenomenon that is also best depicted on a continuum. Immersion is a particularly notable aspect of the metaverse in relation to the topic of extremism and will be expanded upon later in our discussion. At one end of a continuum, immersion may be leveraged to showcase propaganda in an emotionally evocative and cognitively powerful manner, yet at the other, a simple digital overlay (i.e., augmented reality) may provide a user with guidance on which door leads to an exit following an attack.

Although competing labels continue to emerge and language also evolves, following a similar trajectory of the internet and personal computing devices, the expansion and ubiquity of what we now call the metaverse will impact nearly every aspect of society and human interaction. Although the notion of the metaverse reached an unsustainable fever pitch in 2022, companies continue to recognise that integrating metaverse technologies into daily lives is unavoidable. A recent report by McKinsey, for example, estimated a five trillion-dollar impact by 2030.[8] As such, although the broad hype of the metaverse has died down, substantive interest from major players in the technology market continues. Citing a recent *Harvard Business Review,* it appears that "Yes, the metaverse is still happening".[9] Most relevant to our discussion here, however, this trajectory both directly and indirectly links to how violent extremist organisations can recruit, plan, and finance their operations by leveraging this ecosystem.

Implications of the Metaverse in the Terrorism and Violent Extremism Context

Given the emergence of metaverse and related extended reality (XR) technologies, we have outlined some of the key features and mechanisms by which these phenomena are structurally different from traditional web-based platforms and experiences. In this section, we shift the focus from understanding what the metaverse is to the implications of this new landscape for violent extremist actors, groups, and organisations. Building off early initial efforts[10] and congruent with recent reviews[11], we offer at least six ways in which the metaverse may be exploited by terrorists to augment their operations and pursue their strategic objectives: (1) radicalisation, (2) recruitment and member selection, (3) operational training and planning, (4), target selection, (5) finance, and (6) malevolent creativity.[12] In such a discussion, it is important to acknowledge the forward-learning nature of this discussion, identifying the potential for malign application in the emerging threat landscape.[13]

Radicalisation

Online radicalisation occurs by means of the internet, social networking sites, and other forms of online communication and reflects a process through which individuals or groups are exposed to and begin to internalise violent extremist beliefs, which may manifest in behaviour and attitudes.[14] There is a wide range of behavioural influence tactics and tools that are subsumed into online radicalisation, which some have tried to delineate between instrumental (e.g., training manuals, and funding) and communicative (e.g., disseminating information, and recruitment). Others have delineated radicalisation as occurring through several types of interactions, such as sharing information that reinforces prior beliefs; disseminating propaganda with additional material support; seeking legitimisation of future attacks; or attempting to recruit.[15] The immersive environment of the metaverse means that interactions may be more effective than traditional online radicalisation via social media or the dark web. A report by PWC, for example, revealed that VR – compared to traditional video conferencing – resulted in greater emotional connection, focus, and confidence.[16] Other studies on VR and interaction highlight reports of higher social connection as well.[17]

Extended reality offers capabilities for making these interactions more personalized and emotionally evocative. Given the unique features of Web 3.0, the metaverse, and related XR technologies, extremist content – including propaganda or disinformation – can be created and disseminated quickly and effectively,[18] and with fewer established mechanisms for content moderation and monitoring. With the advent of realistic and natural-looking avatars, as well as an influx of data about users on social media (e.g., their interests, photos of their families, etc.), individuals could have a face-to-face interaction in a virtual setting customised to their interests and prior beliefs. Deepfakes – AI-generated images, videos, and voices – as well as realistic-looking avatars, can provoke emotional reactions among users. This may even further reveal the "blurry" intersection between offline and online extremist behaviour.[19] Technological advances afford additional opportunities for realistic interactions and provide a stronger foundation for cultivating influence. These can be generated quickly and customised to increase susceptibility to radicalisation.

Recruitment and Member Selection

Although organisations differ in their goals, be they for good or ill, all face common challenges.[20] One of those ubiquitous challenges is deciding who should join the organisation and what role they should play in it. Hunter and colleagues[21], for example, outline the tools used by al-Qaeda in recruiting and selecting members for their terrorist organisation. These tools and techniques (e.g., interviews, life history, and online applications) mirror those used by many, if not most, corporations. Given the parallels, it seems reasonable to consider how metaverse tools used to select members in traditional organisations could also be adopted by extremists.

Admittedly simplifying for space constraints, web-based recruitment processes often follow several distinct phases.[22] First, recruiters who monitor online communities make initial contact with an individual, usually of a vulnerable population (e.g., individuals seeking community). Next, the recruiter invites the individual to a micro-community, where they share information in a private community and reinforce feelings of belonging or exclusivity among members.[23] This is where, historically, the interaction has involved voice or video conversation. Interactions using technology in the metaverse ecosystem, however, provide unique and increased opportunities for interaction while leveraging the cost-effective (e.g., not requiring the cost of travel while still experiencing nearly in-person equivalent interaction) and customisable (e.g., avatar choice, and location choice) options, made available via digital content. As noted earlier, these immersive experiences can be superior to voice or video engagement for generating feelings of presence and closeness.[24]

Moreover, younger users are more likely to engage in virtual and augmented reality learning and coordination, allowing a wider range of recruits to be accessed quickly.[25] To provide context on these trends, 70 percent of US children aged 9-12 play the game Roblox, with a whopping 70 million daily users worldwide.[26] Roblox has also recently entered the VR space as well, highlighting the trend toward immersive spaces.[27] These and future advances in technology will remedy constraints on traditional forms of recruitment, as recruiters rely on emerging virtual online communities to seek out and connect with individuals in search of connection and community. In the case of Roblox, there are already issues with extremist content – a trend likely to increase as the user base expands.[28]

Operational Training and Planning

There are several features to the metaverse and other extended reality technologies that may afford extremist organisations new capabilities related to operational training and planning. Training aids the acquisition of knowledge and strengthens skills, as well as captures cognitive, behavioural, and affective development.[29] In the context of violent extremism, following radicalisation and recruitment, virtual learning occurs to socialise and instruct behaviours, such as accessing ideological content, opting for violence, choosing a target, preparing an attack, overcoming anticipated hurdles, and coordinating with fellow members (e.g., security measures).

Traditional means of operational teaching have taken place in various terrorist training camps around the world, such as the Khaldan Training Camp in Afghanistan.[30] Examples of common training outcomes include (but are not limited to), how to mount a rocket launcher onto a truck, how to build an improvised explosive device, how and where to launder money, how to successfully surveil, and more. Many such camps share a number of common characteristics. First, they are geographically isolated to build group identity and cohesion (and avoid detection). Second, these are often under sustained pressure as regular targets of directed counter-terrorism initiatives. Finally, these camps require easy access to weapons, ammunition, food, and water.[31] These characteristics pose constraints to individuals wanting to join an organisation from across the world. However, the advent of social media, the metaverse, and related technologies have created new opportunities for distance learning approximating "hands-on" teaching and development.

To be clear, the internet has already created robust opportunities for online engagement with extremist organisations. However, Web 2.0 applications limit access to tactical training required to execute an attack. Reading a training manual is not the same as multiple people walking through an interactive digital version in real-time. In contrast, immersive environments, full-body haptic suits, and augmented reality can allow individuals to train together despite their geographic location. Consider a scenario in which an individual visits a shooting range to practice shooting their desired target (in the form of augmented reality holograms) instead of paper target practice. In a different scenario, an individual practices loading and shooting semi-automatic weapons within a virtual reality immersive shooting range while wearing a full-body haptic feedback suit. In both examples, the individuals are tactically and operationally preparing themselves to shoot a weapon correctly and accurately, as well as desensitising themselves to real-world outcomes. Immersive technology, as well as haptic feedback and extended reality, create new opportunities and remedy constraints to tactical, operational, and affective training activities for extremist organisations.[32]

Second, terrorist organisations can use virtual spaces to plan and prepare for attacks in the physical world. For example, using a VR headset, an individual can visit a virtual location (i.e., a "digital twin") of a critical infrastructure target, such as a power substation or water treatment

facility. During their virtual visit, a prospective attacker can determine the potential for harm to surrounding infrastructure, and the best place to target based on traffic, flow, and the scale of the target. Planning is an essential step in the attack process, where they begin to decide whether their goals will be met by virtually exploring options. Because they are in an undisclosed location, wearing a headset, and using a publicly available app, this type of selection planning goes unnoticed and cannot be reported.

Target Selection

Related to the above, extremist and terrorist organisations choose an attack location as a function of their strategic goals, which include recruiting, inciting fear, and maximising harm. In this case, the rise of the metaverse as an ecosystem allows for new targets to emerge within these digital spaces. Ultimately, terrorists use violence as a vehicle for communicating a political message and driving social and political change.[33] Targets are selected carefully and strategically to align with the perpetrator's desired outcomes, which requires close attention to the political, social, and symbolic value of a target.[34]

The metaverse and related technologies will likely affect target selection in at least two ways. First, terrorist organisations can choose virtual targets, such as digital twins of sacred spaces (e.g., virtual Mecca), or municipal buildings (e.g., virtual embassies and police stations). These opportunities are readily available in virtual environments, as there is very little infrastructure for preventing such attacks. As a recent example, the opening of a Holocaust Museum in the online space Fortnite had to be delayed due to threats of harm to the space.[35] These spaces afford individuals the opportunity to travel or visit museums from the comfort of their homes. However, as the example above highlights, it also presents vulnerabilities to places and objects that are meaningful to individuals. For example, the Virtual Black Stone project created the digital twin of Mecca, the holiest city in Islam.[36] This initiative allows users who have purchased a VR headset (or "Kaaba glasses") to participate in communal live streaming of prayer, and virtually touch the Black Stone or other three-dimensional replicas.[37] The blurring of digital and physical worlds will result in more people transferring to the metaverse to visit digital replicas of vacation destinations, museums, and places of worship. As these soft targets enter the metaverse more readily and with little to no protection, they become the newest grounds for a potential act of violence.

Finance

Terrorist and extremist organisations raise money to conduct their operations and exist as an organisation. Historically, these organisations have raised money from a variety of sources: state sponsorship, theft, international smuggling, drugs, extortion, money laundering, and donations. These funds are used to build training camps, provide food and housing to members, pay salaries, and acquire guns, explosives, triggers, training simulations, fake documents, and technology-mediated communication.[38] The emergence and widespread use of cryptocurrencies and NFTs, in particular, serve as the foundation for how organisations can use the metaverse and related technologies to move money and generate revenue (and some already are doing this). More directly, as a digital ecosystem, the metaverse is built on blockchain and cryptocurrency, meaning that concerns about these finance tools have even greater applicability in the metaverse.[39]

The metaverse may prove an ideal environment for the laundering and transfer of funds controlled by terrorist actors. For example, laundering money via NFT art sales is ambiguous and lucrative, whereby substantial money can be exchanged, without regulation and with limited risk.[40] Transferring money within Web 3.0 allows for greater anonymity, lower fees, and minimal physical infrastructure. Generating revenue will likely mirror established approaches but capitalise on unique features of extended reality technologies. Donation pools will increase,

as methods of sending money can go unnoticed. For instance, imagine a teenager is radicalised after spending time in VR and decides to send money to a foreign terrorist organisation. Instead of using PayPal, which exists on a centralised platform, they decided to anonymously send money via decentralised Web 3.0. Other methods, including scams, identity theft, and extortion, will likely use AI, deepfakes, NFTs, and biometric data.[41]

Malevolent Innovation and Creativity

Although creativity and innovation have traditionally been depicted as more positive or benevolent phenomena, researchers have recently begun to acknowledge that malign actors are also quite capable of novel ideation and implementation.[42] Malign and malevolent creativity may come in a variety of forms, yet technology is often a means by which novel attacks and other kinds of harm are deployed.[43] Along these lines, researchers have examined the impact technology can have on shaping creativity and innovation. Although there is some variability in the precise nature of the impact, technological advances have generally been linked to enhanced creative production.[44] As a specific example, in a sample of engineering students, Starkey and colleagues examined virtual vs. physical product dissection, where participants disassembled products to learn about inner workings and mechanisms, prior to generating new mechanical designs for a dart gun. Comparing the creativity of the dart gun models developed, the researchers found that virtual product dissection resulted in greater creativity than physical product dissection. That is, manipulating products in a virtual environment produces more creative ideas than manipulating physical products.

The emergent argument here is that advances in technology serve as the backbone to how the metaverse will result in greater potential for novel idea production. Most relevant to the present effort is that this appears true for both malevolent and benevolent forms of creativity, although a few points are warranted when discussing malevolent forms of creativity. The first is that increased anonymity linked to the metaverse will allow for the sharing of harmful ideas that are novel, further increasing this form of creativity. Consider, for example, the case of Seif Allah Hammami, who learned of developing the poison ricin from encrypted chats on Telegram.[45] The second is that the metaverse will allow for the prototyping and testing of novel attacks or approaches in digital twin contexts. That is, as the metaverse continues to map the physical world and create a digital analogue, there will be the potential to engage in simulations using those digital twins. As exploration and testing are critical to successful innovation, the metaverse will allow for novel ideation and development in ways not possible prior to the ubiquity of such technology. Although other examples exist, the takeaway here is that creativity and innovation will increase with advances in metaverse technology. This trend will be true for both benevolent and malevolent forms, with non-trivial advances unique to more malevolent innovative outcomes.

How and Why Immersive Metaverse Experiences Will Uniquely Create In-Roads for Violent Extremism: Social and Psychological Mechanisms

In the previous section, we offered ways that the metaverse may be leveraged by extremists to further violent ends. Yet, to better understand the vulnerabilities of users while in the metaverse, it is necessary to detail the mechanisms by which this emerging ecosystem can have a unique impact. Although admittedly not comprehensive due to space constraints, we draw on theories and mechanisms in the fields of psychology and computer science to provide guidance on how and why the metaverse represents an area worthy of consideration by terrorism researchers. More directly, the state of science in these fields offers a deeper understanding of how, and

to what extent, the vulnerabilities identified in earlier sections can affect users in a digital world. Moreover, by understanding these mechanisms, researchers and practitioners can more effectively and directly combat attempts to leverage the capabilities of the metaverse applied for malign ends.

Engagement in a Mixed Reality World – Potential Implications

A key to understanding the metaverse is recognising the potential for immersive experiences uniquely offered by XR technology, and VR in particular. As noted earlier in our discussion, immersion in the digital world is the sense of being in the virtual setting, a phenomenon defined by both technological and user-focused contributions (e.g., custom avatar creation) in the metaverse. High-speed fifth-generation internet, artificial intelligence-powered tools, advances in lenses, and cloud computing can optimise immersion, as well as virtual avatars that deploy similar human-like behaviours and attitudes. These tools, as well as digital twinning with environments that look and feel natural to the physical world aid interconnected experiences on metaverse and extended reality platforms. Users' minds and bodies become unable to differentiate between physical and digital experiences, as they all feel real when immersed. More directly, neuroscientists have begun using functional magnetic resonance imaging (fMRI) machines to examine participants' brain while using these devices, revealing similar patterns of stimulation when using metaverse devices as compared to physical experiences.[46] In other words, emerging research indicates that as metaverse devices advance, our brains cannot distinguish between virtual and physical realities. Consider the capturing of 360-degree video by the terrorist group the Houthis mentioned at the outset. An individual viewing that event in an immersive device would form memories and sensations akin to experiencing that attack as if they were a member boarding that ship via helicopter. This is not to suggest full equivalence of such experiences, of course, but rather to underscore that engagement using XR devices would represent a non-trivial escalation from historical means of sharing terrorist propaganda. Colloquially speaking, it's a notable step-up from watching disinformation and propaganda videos on cozy.tv or kick.com.

Empathy and Perspective Taking

Extending the conversation from above, due to the immersive nature of a fully realised, 3D digital world, users may feel notable empathy towards other avatars or digital representations, thereby offering another tool to be leveraged by malign actors. That is, VR, AR, and XR devices afford greater immersion and challenge the brain's capacity to distinguish digital individuals from physical ones. As such, seeing a digital avatar will elicit empathy on par with a person standing in front of you. Empathy is comprised of two subdimensions: cognitive empathy and emotional empathy.[47] Cognitive empathy, the ability to understand the feelings of others, is elicited by conscious and effortful mental processes, whereas emotional empathy is the ability to feel concern for others and occurs automatically through unconscious processing.[48] This combination of explicit and implicit processes is described as a dual-process system by psychologists. In the context of VR, evidence suggests that such experiences can improve emotional empathy.[49] This occurs because the immersive nature of VR allows explicit presentation of thoughts and feelings of others eliminating the need to engage in conscious mental effort. Through implicit, emotional empathy, VR users can feel for others, but are not required to think about the perspectives of others through cognitive empathy consciously.

Given such implicit empathy, users subjected to emotion eliciting content will feel deep and genuine concern for what they witnessed. Eliciting empathy and concern are typically pro-social human emotions, but the ease of doing so using immersive technologies coupled with the

increased range of audiences are also conducive to fear garnering tactics used by extremists. Eliciting fear through violence is not novel to the metaverse and, instead, represents an extension of current tactics on the part of extremist organisations. ISIS, for example, prioritises inciting fear through violent propaganda on YouTube.[50] Using these methods of propaganda distribution, terror groups share graphic acts of violence, such as beheadings.[51] However, improvements to video fidelity and a sense of immersion afforded by metaverse technologies have the potential to amplify this effect in a non-trivial way. The immersion triggers deep and automatic empathetic concern before conscious mental effort even occurs. That is, even a short exposure to violent imagery could instil fear before the propaganda is removed. In the case of deepfakes, fear tactics can target individuals by modifying the appearance of victims to appear similar to onlookers (i.e., seeing oneself or a family member harmed or tortured). The immersive nature combined with self-prioritising processes likely means the psychological response of fear is more rapid than that provoked by preceding forms of propaganda.[52]

Copresence and Social Presence

When describing immersion in a virtual environment, computer scientists rely on psychological copresence and social presence to describe interacting with other users in the environment. More specifically, these phenomena provide scaffolding for forming relationships and socialising in a digital environment. Copresence is the sense of mind and connection with an individual, leading to mutual perception of each other.[53] Social presence is the degree of salience between individuals in an interaction. It is described as the feeling of psychological proximity, closeness, connectedness, and intimacy with one another via the medium of communication.[54] When avatar behavioural realism and visual realism are not aligned (e.g., delays in avatar movements or an avatar displays inappropriate facial expressions during a conversation), the perception of social presence is lower.

5G network speed and dissemination of information facilitate a greater sense of presence and copresence when users are immersed in a digital environment. Both phenomena are necessary factors for a user to feel and sense they are truly in their virtual world. It is impossible for a user to embody their avatar and immerse themselves without these phenomena present, as they explain why and how users feel connected to their digital environments and can build relationships with other digital users.

The importance of copresence and social presence to extremism has been touched on in our earlier section, but examples include activities such as recruitment, where a leader would be able to remotely connect with a potential member in a way that feels immediate, rich, and immersive due to the capabilities of emerging metaverse technologies. That is, advanced technological capabilities can make recruits feel as if they are spending time with a terror group in real-time. Similarly, the ability to plan and coordinate attacks from a distance is also afforded due to copresence and social presence. As speed and technology improve, the ability to practice and coordinate specific timing of events is also increased. As a final illustration, the sense of connection to a larger group and being part of a community is facilitated with this technology and moves beyond a typical listserv, chatroom, or even video call. In other words, members can meet and build kinship remotely in a way that is similar to – and with the benefits of – an in-person event, while limiting exposure to an attack or entities (e.g., the FBI) creating records of meeting attendance (if anonymity protocols are applied).

Sense of Embodiment

Moving from perceiving others in the environment to feeling connected to one's digital self, sense of embodiment (SoE) describes the unconscious process of feeling one's own body.[55] Cognitive neuroscientists describe this sensation as how the brain expresses the body related

to having, being in, and controlling a virtual body. Computer scientists suggest SoE is related to bottom-up information (e.g., visual and tactile) and top-down information (e.g., cognitive processes that modulate processing sensory stimuli). To illustrate these information processes, Botvinick and Cohen conducted experiments to investigate the rubber hand illusion. The core function of these experiments was to induce the embodiment of an artificial hand. During the experiment, participants were placed in front of a rubber hand while their hand was obstructed from view. The participant's hand was then stroked with a paintbrush while the rubber hand was also being stroked. Participants began to take ownership of the rubber hand in front of them after some time.[56] When that hand is attacked, genuine fear and protection of that hand occurs. Participants gasp, snatch their hands away, and spike physiological stress responses. They know their hand is safe, but the brain builds connections that are quite real to the body. The implication for terrorism is that as users engage with metaverse devices, users' brains begin to inform the body that the experience has real danger and the experience, physiologically speaking, is nearly as real as a physical experience.

There are three classes of embodiment: self-location, agency, and body ownership.[57] Self-location is related to a user's point of view, which can determine the spatial relationships of one's avatar and their virtual body.[58] More specifically, the sense of self-location is greater in first-person than in third-person views. Put simply, the sense of self-location impacts how a user perceives themselves to be located in their digital environment. Sense of agency is related to one's ability to control one's avatar. Congruent physical and virtual body movements contribute to a high sense of agency, whereas discrepancies or keyboard-controlled movements tend to decrease one's sense of agency.[59] Agency plays an important role in recognising one's actions and impacts ownership of digital selves.[60] One's self-location and agency influences their body ownership, or sense of ownership, over their avatar. Congruent visual, motor, and tactile movements from a first-person point of view impact one's sense of ownership to the greatest extent. For example, when users have an extra body part, say a virtual tail, their sense of ownership is higher when they can control it by moving their hips.[61] Together, the sense of embodiment describes the sensations related to having, being located in, and controlling a virtual body.[62]

The illusionary ownership of one's avatar, achieved by a synchronous first-person point of view, is also described as a body swap illusion. This phenomenon describes users perceiving their physical bodies as swapping with their digital selves.[63] Body swap illusion can be induced by placing individuals in a multi-sensory stimulation in a first-person perspective. Keizer et al. induced the illusion with participants suffering from anorexia nervosa. Throughout the study, participants perceived stimulation (e.g., haptic feedback) on their physical bodies while viewing the same stimulation on their virtual avatars. Participants of these studies reported decreased body-size overestimation. When manipulating visual and auditory feedback, body swap illusion can be induced, potentially impacting users' behaviour.[64] Although these phenomena could be leveraged by malign actors in a variety of ways, several come to mind initially. The first is by facilitating a sense of dehumanisation by placing recruits or members into avatars that promote a loss of individuality (e.g., making all recruits look the same). This dehumanisation process is used by terrorist groups to allow greater control over members for acts of violence.[65] A second illustration would be placing a member in the avatar of a victim who was attacked by an adversary. This would allow a member to experience that attack and develop an intimate desire for justice or revenge. Imagine, for example, experiencing the attack on a wedding procession in Yemen from the eyes of the bride and the impact that would have on a member then tasked with retribution.[66]

Proteus Effect

When a user feels a sense of ownership or body swaps with their avatar, behavioural or attitudinal changes are defined as the proteus effect. The proteus effect explains an individual's likelihood to conform to how they believe their embodied avatar should act.[67] The effect received its name from the Greek god Proteus, known for his ability to change shape and alter reality. Because users often represent themselves differently online, their behaviours may subsequently change to match their new, desired appearances.[68] Rooted in self-perception theory, users can customise their avatars' appearances, leading users to choose their appearances and subsequent attitudes and behaviours. Some studies suggest that users who perceive their avatars as being attractive act more extroverted and friendly, and taller avatars were perceived as more confident and in positions of power.[69] The proteus effect, a manifestation of body ownership, serves as a foundational aspect of immersive experiences.

The key here, from a terrorism perspective, is that the proteus effect is a lasting effect outside of the immediate virtual reality experience. That is, beliefs, perceptions, and attitudes persist post-engagement. As such, this phenomenon could be leveraged by malign actors by using metaverse technologies as a starting point for indoctrination, recognising that those perceptions will persist once they stop using those technologies. That is, the proteus effect illustrates how immersive experiences and their impacts do not end once the devices are removed.

Place Illusion and Plausibility Illusion

An extension to the proteus effect involves place and plausibility illusions. Fully immersive experiences cause the lines between digital and physical worlds to blur, resulting in the belief that one is actually in the digital environment and interacting or connecting with others. Along these same lines, users start to believe that the things they see or experience actually happen. Similar to waking up from a bad dream and thinking about it throughout the day, situations or scenarios that occur in an immersive digital environment can have lasting effects on witnesses. Consider the drone attack on the wedding processional noted earlier and the long-term effect experiencing that event in an immersive environment would produce.

Formally, place illusion is the belief of being in a virtual environment despite the user knowing they are not there.[70] Similar to the body swap illusion, users can look down and see their avatar's body. There is no direct way to measure place illusion, but some researchers have compared responses between digital and physical environments.[71] Plausibility illusion is defined as the belief that a scenario in a digital environment actually occurred.[72] This illusion happens when events are not directly caused by the user and their own sensations, such as another avatar speaking or walking towards the user's avatar. These different immersion illusions can cause users to become vulnerable to their digital environments. For example, a woman reported being virtually sexually assaulted by a group of 3-4 avatars with male voices while beta testing the VR platform Horizon Worlds. Due to the nature of virtual reality, the user could not differentiate their experiences between physical and virtual.[73] Explained by the place and plausibility illusions, users feel as though their virtual experiences really happened to their physical bodies. Taken together, these phenomena outline the mechanisms by which the metaverse and related technologies are a step forward in the potential for malign application by terrorists.

Limitations

Although our review here provides an overview of key features of the metaverse, related technologies, and mechanisms for malign application, several limitations should be borne in mind. First, although many organisations have dedicated significant resources to building the metaverse as an ecosystem, there is some indication of shifting interest. The company

Meta (formerly Facebook), for example, has recently shifted resources from VR/XR/MR to AI. Although these trends are notable, they are also expected as interest waxes and wanes in new technology. Moreover, the investment and focus on AI are not mutually exclusive to the metaverse, as AI may similarly be leveraged by malign actors in ways related to (e.g., creating 3D environments quickly and easily) and unique from the metaverse itself (e.g., flying autonomous drone swarms).[74] Tempered views are warranted, however, in predicting the future of digital and physical intersections. Second, given space constraints, we were not able to detail all psychological mechanisms by which the metaverse may be leveraged by malign actors. Although we hope that our discussion provides a starting point, these mechanisms are not comprehensive and as such should be viewed as a limitation. Finally, many of the examples provided are speculative in nature, drawing on current trajectories and pairing them with what is likely in the future. Nonetheless, our work here is forward-leaning and should be viewed as such, conceding the likelihood of proving incorrect in some instances.

Future Research

When discussing what might be done to limit the range, reach, and impact of extremist organisations it is clear that a number of knowledge gaps remain. Although space does not permit a discussion of every gap, we offer two areas that warrant consideration in future efforts. The first is an examination of the differences between domestic and foreign actors. As an analogy, we may turn to drone use capability and how drones have been adopted by terrorist groups across the globe. Conceding a nuanced history, the success of commercial drones in delivering lethal payloads in the Middle East paired with their commercial availability now makes them appealing to extremists in the US.[75] That is, this technology has emerged as a credible, if not novel, domestic threat despite its use originating outside of the US. Highlighting the unique characteristics and challenges of terrorism in the metaverse. However, this analogy only works when the avatar we might engage within a digital environment may be a neighbour who subscribes to white nationalist ideology or a member of ISIS based in West Africa. Moreover, the digital nature of interaction means that these geographically dispersed groups could find common ground in digital spaces. Stated more broadly, it will be critical to examine differences (if they exist) between how foreign terrorist organisations and domestic violent extremists use the metaverse for malign purposes, as well as how these groups may blend in the often anonymous, richly connected digital environment.

Second, we offer that the emergence of dynamic, communication-rich, and deeply embedded forms of technology – such as the metaverse – may result in their own form of ideological rejection. Like racially and ethnically motivated violent extremists (REMVE), Salafi Jihadists, or anti-government, anti-authority violent extremists (AGAAVE), we may see an "anti-metaverse" ideology formed. Ted Kaczynski, also known as the Unabomber, has either inspired or been linked to groups and communities such as anarchists, neo-Luddites, primitivists, and ecofascists. In his manifesto, *Industrial Society and Its Future*, he makes a number of arguments including that humans are psychologically and biologically maladapted to a society that is grounded in a technological system. This sentiment is evident in some circles today, as modern groups gravitate toward similar ideologies, albeit in less violent ways. Indeed, there is a growing sentiment among some youth groups that refer to themselves as Luddite teens or the Luddite club who are actively opposed to the rich forms of technology that continue to evolve and permeate our lives.[76] Thus, it will be critical that those in law enforcement and homeland security consider how current extremist groups may leverage the metaverse, while also recognising that the very existence of the metaverse may result in extremists seeking to push against it.

Summary and Concluding Comments

To summarise, this exploration of the metaverse's implications for violent extremism and terrorism underscores the urgent need for interdisciplinary research and proactive measures. Our review highlights the metaverse's potential to revolutionise not only societal interactions but also the methods by which extremist ideologies are propagated and operationalised. By defining the metaverse, illustrating its use in extremist activities, and delving into the psychological underpinnings that make such technologies potent tools for radicalisation and terror, we lay the groundwork for understanding the emerging threat landscape.

Key themes include the unique affordances of the metaverse for recruitment, planning, and execution of extremist acts; the role of immersive technologies in enhancing radicalisation and operational training; and the novel challenges these developments pose to content moderation, security, and counter-terrorism efforts. The call for future research emphasises the importance of distinguishing between the uses of the metaverse by different extremist groups, addressing the originality bias in threat assessment, and considering the potential for anti-technology extremism. This analysis not only illuminates the complexities of the metaverse as a double-edged sword but also underscores the critical need for collaborative efforts to navigate the challenges it presents to global security. The metaverse as a concept is equally amorphous as it is complex. It continues to evolve as an idea, yet there is consensus that it will impact the lives of many. We stand now with the initial surge of interest quieting and the real process of technological change beginning. Extended reality hardware will become embedded in our lives, and all forms will become cheaper and easier to use. Software will be developed and, with the support of AI, also be easier to deploy by an army of content makers. Without expressly knowing it, AR and VR will quietly seep into our lives. With that immersion and embeddedness comes access. Doctors can more readily fix our bodies, families can connect in ways unimaginable a generation prior, instructors and professors can show us rather than lecturing to us. And of course, malign actors will have a new platform and a novel tool in their behavioural influence arsenal. No meaningful force has ever landed squarely on the side of benevolence, be it gunpowder, nuclear fission, or the printing press. Rather, it is incumbent to embrace and protect those with benevolent aims and prepare for those with malevolent intent. We hope this discussion moves the needle on both.

Dr Sam Hunter is a Regents-Foundation Professor of Organizational Psychology at the University of Nebraska at Omaha and the Head of Strategic Initiatives at the National Counterterrorism, Innovation, and Technology (NCITE) centre of excellence. His primary areas of research include leadership and innovation with a particular focus on malign application of each.
Twitter: @dr_samhunter

Alexis d'Amato is an Industrial and Organizational Psychology PhD student at the University of Nebraska at Omaha. She holds a Bachelor of Science in Marketing and Management from the University of Nebraska at Omaha. Her research interests include conventional and malevolent creativity and creativity training. Twitter: @alexis_damato

Dr Joel Elson is an Assistant Professor of IT Innovation at the University of Nebraska at Omaha and serves as a Principal Investigator at the National Counterterrorism Innovation, Technology, and Education (NCITE) Centre. His research focuses on human-computer interaction, mixed-initiative teaming, and cyber-influence, particularly exploring trust and its impact on behaviour and decision-making. Elson specialises in eye-tracking instrumentation to measure intangible latent

constructs. He has collaborated with local businesses, Fortune 500 companies, and government agencies, including the US Department of Defense and the US Department of Homeland Security, conducting applied research on innovative technology for counter-terrorism and identifying emerging threats.

Dr Austin C Doctor is the director of counter-terrorism research initiatives at the National Counterterrorism Innovation, Technology, and Education (NCITE) Center, a Department of Homeland Security Centre of Excellence, and a political scientist at the University of Nebraska at Omaha. He has served as a non-resident fellow with the Modern War Institute at the United States Military Academy at West Point as well as the National Strategic Research Institute, a Department of Defense University Affiliated Research Center. He earned his PhD at the University of Georgia. His research focuses on militants, terrorism, and emerging threats. Twitter: @austincdoctor

Averie Linnel is an Industrial and Organisational Psychology PhD student at the University of Nebraska at Omaha. Her research interests include conventional and malevolent creativity. Twitter: @AverieLinnell

Acknowledgement & Disclaimer: Portions of this manuscript are based on work supported by the US Department of Homeland Security under Grant Award Number, 20STTPC00001-02. The views and conclusions included here are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the US Department of Homeland Security or the University of Nebraska System.

Endnotes

1 Lik-Hang Lee, Tristan Braud, Pengyuan Zhou, Lin Wang, Dianlei Xu, Zijun Lin, Abhishek Kumar, Carlos Bermejo, and Pan Hui. "All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda." *Journal of Latex Class Files,* 14, no. 8 (September 2021): 1-66.

2 Ibid.

3 Ian Talley, "Islamic State Turns to NFTs to Spread Terror Message." *The Wall Street Journal*, 6 September 2022, https://www.wsj.com/articles/islamic-state-turns-to-nfts-to-spread-terror-message-11662292800.

4 Y. H. Chou, Carol P. Weingarten, David J. Madden, Allen W. Song, and N. K. Chen. "Applications of virtual reality technology in brain imaging studies." *Virtual Reality in Psychological, Medical and Pedagogical Applications, ed. C. Eichenberg (Croatia: InTech)* (2012): 203-228; Farzin Hajebrahimi, Halil Aziz Velioglu, Zubeyir Bayraktaroglu, Nesrin Helvaci Yilmaz, and Lutfu Hanoglu. "Clinical evaluation and resting state fMRI analysis of virtual reality-based training in Parkinson's disease through a randomized controlled trial." *Scientific Reports* 12, no. 1 (2022): 8024.

5 S. Joel Elson, Austin C. Doctor, and Samuel T. Hunter. "The Metaverse offers a future full of potential–for terrorists and extremists, too." *The Conversation*, 7 January 2022, https://theconversation.com/the-metaverse-offers-afuture-full-of-potential-for-terrorists-and-extremists-too-173622; Gabriel Weimann and Roy Dimant, "The Metaverse and Terrorism: Threats and Challenges." *Perspectives on Terrorism* 17, no. 2 (June 2023): 92-107; Suraj Lakhani, "When Digital and Physical World Combine: The Metaverse and Gamification of Violent Extremism." *Perspectives on Terrorism,* 17, no. 2, (June 2023): 108-178.

6 Jiajing Wu, Kaixin Lin, Dan Lin, Ziye Zheng, Huawei Huang, and Zibin Zheng. "Financial Crimes in Web3-empowered Metaverse: Taxonomy, Countermeasures, and Opportunities." *IEEE Open Journal of the Computer Society* 4 (2023): 37-49; Jade Hutchinson, Julian Droogan, Lise Waldek, Jade Hutchinson, and Brian Ballsun-Stanton. "Violent extremist & REMVE online ecosystems: Ecological characteristics for future research & conceptualization." *Resolve Network* (2022): 6-31.

7 Sophie Morosoli, Peter Van Aelst, Edda Humprecht, Anna Staender, and Frank Esser. "Identifying the drivers behind the dissemination of online misinformation: a study on political attitudes and individual characteristics in the context of engaging with misinformation on social media." *American Behavioral Scientist* (2022): 1-20; Richard Skarbez, Missie Smith, and Mary C. Whitton. "Revisiting milgram and kishino's reality-virtuality continuum." *Frontiers in Virtual Reality* 2 (March 2021).

8 McKinsey (2022) "Value creation in the metaverse, 2.02/2023." McKinsey & Company, https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/valuecreation-in-the-metaverse.

9 Deborah Piscione and Drean, Josh. "Yes, the metaverse is still happening." *Harvard Business Review* (May 2023).

10 See Elson, et al. (2022)

11 See Weimann and Dimant (2023); Lakhani (2023)

12 Bajwa, Aman. "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; Weimann and Dimant (2023); Lakhani (2023)

13 Weimann and Dimant (2023); Lakhani (2023)

14 Michael Breazeale, Erin G. Pleggenkuhle-Miles, Mackenzie Harms, and Gina Scott Ligon. "The dark side of CRM: Brand relationships and violent extremist organisations," in *The Dark Side of CRM*, edited by Bang Nguyen, Lyndon Simkin, and Ana Isabel Canhoto, 192-214. Routledge, 2015; Maja Golf-Papez, Jonas Heller, Tim Hilken, Mathew Chylinski, Ko de Ruyter, Debbie I. Keeling, and Dominik Mahr. "Embracing falsity through the metaverse: The case of synthetic customer experiences." *Business Horizons* 65, no. 6 (2022): 739-749; Peter R. Neumann, "The trouble with radicalization." *International Affairs* 89, no. 4 (2013): 873-893; Joe Whittaker, "Rethinking online radicalization." *Perspectives on Terrorism* 16, no. 4 (2022): 27-40; Bart Schuurman, "Non-Involvement in Terrorist Violence." *Perspectives on Terrorism* 14, no. 6 (2020): 14-26.

15 Austin L. Wright, "Terrorism, ideology and target selection." *The Pearson Institute Discussion Paper,* no. 9 (2013): 1-31; Paul Gill, Emily Corner, Amy Thornton, and Maura Conway, "What are the roles of the Internet in terrorism? Measuring online behaviours of convicted UK terrorists." *VOX Pol* (2015):10-34.

16 PWC Network. "What Does Virtual Reality and the Metaverse Mean for Training." https://www.pwc.com/us/en/tech-effect/emerging-tech/virtual-reality-study.html. Accessed 30 January 2024.

17 Bronwyn, Tarr, Mel Slater, and Emma Cohen. "Synchrony and social connection in immersive virtual reality." *Scientific Reports* 8, no. 1 (2018): 3693.

18 Don Fallis, "The varieties of disinformation," in *The Philosophy of Information Quality*, edited by Luciano Floridi and Phyllis Illari, 135-161. Switzerland: Springer International Publishing, 2014.

19 Whittaker, (2022): 32; Paul Gill et al., "Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes," *Criminology and Public Policy*, 16(1), (2017): 114.

20 Jacob N. Shapiro, *The Terrorist's Dilemma: Managing Violent Covert Organizations*. Princeton University Press, 2013.

21 Hunter, et al. (2017)

22 J. M. Berger, "Tailored online interventions: The Islamic state's recruitment strategy." *CTC Sentinel* 8, no. 10 (2015): 19-23.

23 Ibid; Martha Crenshaw, "I've Studied Terrorism for over 40 Years. Let's Talk about What Comes Next." *The New York Times*, 10 February 2021, https://www.nytimes.com/2021/02/10/opinion/capitol-terrorism-right-wing-proud-boys.html.

24 Abraham G. Campbell, Thomas Holz, Jonny Cosgrove, Mike Harlick, and Tadhg O'Sullivan. "Uses of virtual reality for communication in financial services: A case study on comparing different telepresence interfaces: Virtual reality compared to video conferencing." In *Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), Volume 1*, pp. 463-481. Springer International Publishing, 2020.

25 Gill, Corner, Thornton, and Conway (2015).

26 Matthew Ball, *The Metaverse: And How It Will Revolutionize Everything*. Liveright Publishing, 2022.

27 Jay Peters, "Roblox is Now Available to Try on Meta Quest VR Headsets." *The Verge*, 2023, https://www.theverge.com/2023/7/27/23810093/meta-quest-roblox-vr-headsets-beta.

28 *The Guardian.* "Online Gaming Platforms Such as Roblox Used as "Trojan Horse" for Extremist Recruitment of Children, AFP warns. https://www.theguardian.com/australia-news/2023/dec/03/online-gaming-platforms-such-as-roblox-used-as-trojan-horse-for-extremist-recruitment-of-children-afp-warns. Accessed 30 January 2024.

29 Den Ladden-Hall, "Russian Teen's Sentence Upheld in Minecraft Terrorism Case." *The Daily Beast*, 17 January 2013, https://www.thedailybeast.com/russia-upholds-sentence-against-teen-who-planned-to-blow-up-fsb-building-in-minecraft.

30 Michael J. Franklin,and Stanley B. Zdonik. "Dissemination-based Information Systems." *IEEE Data Eng. Bull.* 19, no. 3 (1996): 20-30.

31 Ibid.

32 Jakob Fröhner, Gionata Salvietti, Philipp Beckerle, and Domenico Prattichizzo. "Can Wearable Haptic Devices Foster the Embodiment of Virtual Limbs?" *IEEE transactions on haptics* 12, no. 3 (2018): 339-349.

33 Victor H. Asal, R. Karl Rethemeyer, Ian Anderson, Allyson Stein, Jeffrey Rizzo, and Matthew Rozea. "The Softest of Targets: A Study on Terrorist Target Selection." *Journal of Applied Security Research* 4, no. 3 (2009): 258-278.

34 R. Kim Cragin, "Virtual and Physical Realities: Violent Extremists' Recruitment of Individuals Associated with the US Military." *Studies in Conflict & Terrorism* (2022): 1-22.

35 Sarah Cascone, "The Opening of a New Virtual Holocaust Museum in Fortnite Has Been Delayed After White-Supremacist Nick Fuentes Rallied Antisemites to Attack It." ARTNet (August 10, 2023).

36 Gruber, Christine. "Muslims in the Metaverse." *New Lines Magazine*, 30 November 2022, https://newlinesmag.com/essays/muslims-in-the-metaverse/.

37 Ibid.

38 Ibid.

39 Winston Ma and Ken Huang. *Blockchain and Web3: Building the cryptocurrency, privacy, and security foundations of the metaverse*. John Wiley & Sons, 2022.

40 Samuel T. Hunter, Kayla Walters, Tin Nguyen, Caroline Manning, and Scarlett Miller, "Malevolent Creativity and Malevolent Innovation: A Critical but Tenuous Linkage," *Creativity Research Journal* 34, vol. 2 (November 2022): 123-144.

41 Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*. Oxford University Press, 2019.

42 Paul Gill, John Horgan, Samuel T. Hunter, and Lily D. Cushenbery. "Malevolent Creativity in Terrorist Organizations." *The Journal of Creative Behavior* 47, no. 2 (2013): 125-151; Hunter, Walters, Nguyen, Manning, and Miller. "Malevolent Creativity and Malevolent Innovation."

43 Cronin (2019).

44 Joshua Fairchild, Scott Cassidy, Lily Cushenbery, and Samuel T. Hunter. "Integrating Technology with the Creative Design Process," in *Technology for Creative and Innovation: Tools, Techniques and Applications*, edited by Anabela Mesquita, Hershey: IGI Global, 2011, 26-51; Rachel Heinen, Salvatore A. Leone, Joshua Fairchild, Lily Cushenbery, and Samuel T. Hunter. "Tools for the Process: Technology to Support Creativity and Innovation," in *Handbook of Research on Digital Media and Creativity Technologies,* edited by D. Harrison, Hershey: IGI Global, 2015, 374-403; Samuel T. Hunter, Lily Cushenbery, Nicole Ginther, and Joshua Fairchild. "Leadership, Innovation, and Technology: The Evolution of the Creative Process," in *The Evolution of the Creative Process,* edited by Sven Hemlin, Carl M. Allwood, Ben Martin, and Michael D. Mumford, New York: Routledge, 2013, 81-110.

45 Cronin (2019).

46 Y. H. Chou, Carol P. Weingarten, David J. Madden, Allen W. Song, and N. K. Chen. "Applications of virtual reality technology in brain imaging studies." *Virtual Reality in Psychological, Medical and Pedagogical Applications, ed. C. Eichenberg (Croatia: InTech)* (2012): 203-228.

47 Mark H. Davis, "Measuring Individual Differences in Empathy: Evidence for a Multidimensional Approach." *Journal of Personality and Social Psychology* 44, no. 1 (1983): 113-126.

48 Chi-Lin Yu, and Tai-Li Chou. "A Dual Route Model of Empathy: A Neurobiological Prospective." *Frontiers in Psychology* 9 (November 2018): 1-5.

49 Alison Jane Martingano, Fernanda Hererra, and Sara Konrath. "Virtual Reality Improves Emotional but Not Cognitive Empathy: A Meta-analysis." *Technology, Mind, and Behavior* 2, no. 1 (June 2021).

50 Yanyun Wang, Crystal Chen, Michelle R. Nelson, and Sela Sar. "Walk in My Shoes: How Perspective-taking and VR Enhance Telepresence and Empathy in a Public Service Announcement for People Experiencing Homelessness." *New Media & Society*, (August 2022).

51 Simone Molin Friis, "'Beyond anything we have ever seen': beheading videos and the visibility of violence in the war against ISIS." *International Affairs* 91, no. 4 (2015): 725-746.

52 T. B. Rogers, N. A. Kuiper, and W. S. Kirker. "Self-reference and the Encoding of Personal Information," in *The Self in Social Psychology,* edited by R. F. Baumeister (Psychology Press, 1999), 139-149; Frank Tong and Ken Nakayama. "Robust Representations for Faces: Evidence from Visual Search." *Journal of Experimental Psychology: Human Perception and Performance* 25, no. 4 (1999): 1016-1035.

53 Erving Goffman, "International Ritual: Essays on Face-to-face Behavior." *New York: Double Day Anchor Books* (1967); Kristine L. Nowak and Frank Biocca. "The Effect of the Agency and Anthropomorphism on Users' Sense of Telepresence, Copresence, and Social Presence in Virtual Environments." *Presence: Teleoperators & Virtual Environments* 12, no. 5 (2003): 481-494.

54 Ederyn Williams and Bruce Christie, *The Social Psychology of Telecommunication.* London: Wiley & Sons, 1976.

55 Matthew Botvinick and Jonathan Cohen. "Rubber Hands 'Feel' Touch that Eyes See." *Nature* 391, no. 6669 (1998): 756-756.

56 Ibid.

57 Konstantina Kilteni, Raphaela Groten, and Mel Slater. "The Sense of Embodiment in Virtual Reality." *Presence: Teleoperators and Virtual Environments* 21, no. 4 (2012): 373-387.

58 Rebecca Fribourg, Ferran Argelaguet, Anatole Lécuyer, and Ludovic Hoyet. "Avatar and Sense of Embodiment: Studying the Relative Preference Between Appearance, Control and Point of View." *IEEE Transactions on Visualization and Computer Graphics* 26, no. 5 (2020): 2062-2072.

59 Ferran Argelaguet, Ludovic Hoyet, Michaël Trico, and Anatole Lécuyer. "The Role of Interaction in Virtual Embodiment: Effects of the Virtual Hand Representation." *HAL Open Science*, (March 2016): 3-10.

60 Emilie A. Caspar, Axel Cleeremans, and Patrick Haggard. "The Relationship Between Human Agency and Embodiment." *Consciousness and Cognition* 33 (2015): 226-236; Manos Tsakiris, Marcello Costantini, and Patrick Haggard. "The Role of the Right Temporo-Parietal Junction in Maintaining a Coherent Sense of One's Body." *Neuropsychologia* 46, no. 12 (2008): 3014-3018.

61 William Steptoe, Simon Julier, and Anthony Steed. "Presence and Discernability in Conventional and Non-photorealistic Immersive Augmented Reality." *IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*, (September 2014): 213-218.

62 Kangsoo Kim, Celso M. de Melo, Nahal Norouzi, Gerd Bruder, and Gregory F. Welch. "Reducing Task Load with an Embodied Intelligent Virtual Assistant for Improved Performance in Collaborative Decision Making." *IEEE Conference on Virtual Reality and 3D User Interfaces,* (March, 2020): 529-538.

63 Chiara Fini, Flavia Cardini, Ana Tajadura-Jiménez, Andrea Serino, and Manos Tsakiris. "Embodying an Outgroup: The Role of Racial Bias and the Effect of Multisensory Processing in Somatosensory Remapping." *Frontiers in Behavioral Neuroscience* 7, no. 165, (2013): 1-9.

64 Tabitha C. Peck, Sofia Seinfeld, Salvatore M. Aglioti, and Mel Slater. "Putting Yourself in the Skin of a Black Avatar Reduces Implicit Racial Bias." *Consciousness and Cognition* 22, no. 3 (2013): 779-787; Harry Farmer and Lara Maister. "Putting Ourselves in Another's Skin: Using the Plasticity of self-perception to enhance empathy and decrease prejudice." *Social Justice Research* 30 (2017): 323-354.

65 Sara Hamad Alqurainy, Adnan Hamedi, and Abubakar Usman Abubakar. "The road to the slaughter: ISIS process of dehumanizing the enemy." *Opción: Revista de Ciencias Humanas y Sociales* 20 (2019): 757-774.

66 Jeffrey S. Bachman and Esther Brito Ruiz. "The geopolitics of human suffering: a comparative study of media coverage of the conflicts in Yemen and Ukraine." *Third World Quarterly* 45, no. 1 (2024): 24-42.

67 Nick Yee and Jeremy Bailenson. "The Proteus Effect: The Effect of Transformed Self-Representation on Behavior." *Human Communication Research* 33, no. 3 (2007): 271-290.

68 Ibid.

69 Karen Dion, Ellen Berscheid, and Elaine Walster. "What is Beautiful is Good." *Journal of Personality and Social Psychology* 24, no. 3 (1972): 285-290; Young, Thomas J., and Laurence A. French. "Height and Perceived Competence of US Presidents." *Perceptual and Motor Skills* 82, no. 3 (1996): 1002-1002.

70 Mel Slater, "Place Illusion and Plausibility Can Lead to Realistic Behaviour in Immersive Virtual Environments." *Philosophical Transactions of the Royal Society B: Biological Sciences* 364, no. 1535 (2009): 3549-3557.

71 Ibid.

72 Ibid.

73 Hannah Frishberg, "Mother Opens Up About Being 'Virtually Gang Raped' in Metaverse." *New York Post*, 1 February 2022,https://www.nypost.com/2022/02/01/mom-opens-up-about-being-virtually-gang-raped-in-metaverse/.

74 I. B. R. Soto and N. S. S. Leon (2022). How artificial intelligence will shape the future of the metaverse. A qualitative perspective. *Metaverse Basic and Applied Research*, *1*, 12-12.

75 Cronin (2019); Alyssa Sims, "The rising drone threat from terrorists." *Georgetown Journal of International Affairs* 19 (2018): 97.

76 Wright (2013); Philip B. Heymann, *Terrorism, Freedom, and Security: Winning Without War*. Cambridge: MIT Press, 2003.