MALEVOLENT CREATIVITY & THE METAVERSE: HOW THE IMMERSIVE PROPERTIES OF THE METAVERSE MAY FACILITATE THE SPREAD OF A MASS SHOOTER CULTURE

Aman Bajwa, Canadian Association for Security and Intelligence Studies
Vancouver
Canada

Abstract

The innovation of the Metaverse heralds a new milestone in the Information Age as investors move forward with the plan to bring the metaverse to fruition. The metaverse will offer a heightened experience in terms of interactivity, economics, and platform, while paving the way for greater immersion through virtual reality and augmented reality technologies. It is likely that as the metaverse develops, gaming will offer a unique social experience through its features such as virtual worlds. Based on this, it is important for policymakers to look at extremist subcultures that will operate in the metaverse through these virtual features. Due to the role played by fringe subcultures in facilitating the recent mass shooting event in Buffalo, this article aimed to examine the main features of the metaverse and how its immersive properties could influence the creation of future metaversal subcultures that could act as a gateway towards future mass shooting incidents. To that end, it applied the model of malevolent creativity to the extremist use of online spaces to gain insight on how such properties could aid online extremists towards mobilization. Results show that the concatenation of malevolent creativity, innovation, and subcultural extremism may bridge the gap between ideation of mass shootings and mobilization. Based on this, the implication of this research suggests that tech entrepreneurs for the metaverse should be mindful of the risks that disconnection from the real-world society can create for young, isolated users and aim to implement safeguards in integral areas of the metaverse seven-layer chain, such as spatial computing, discovery, and the creator economy.

Introduction

In 1992, science fiction author Neil Stephenson first coined the term *Metaverse* to describe a virtual world in which users immerse themselves with avatars as a means of escaping from their bleak, dystopian, and corporate-controlled reality. At the time of its inception, the book, *Snow Crash*, presented the metaverse as a negative concept correlated with themes such as online addiction, disconnection, and consumerism. Today, however, tech entrepreneurs and futurists are heavily promoting the concept as the next iteration of the Internet that promises interconnectedness and immersion in an online setting facilitated by virtual and augmented reality (Vandhana, 2022). In the metaverse, users will be able to use Virtual Reality (VR) and Augmented Reality (AR) goggles to navigate the online world and essentially be able carry out the same tasks that they would in the real world. This can involve going shopping, going to concerts and sporting events, and going to work in a virtual office setting. In essence, the metaverse will allow the user to take online social connectivity to the next level.

Despite the grandiose claims of its benefits by heavily invested entrepreneurs such as Mark Zuckerberg, very little discussion has revolved around how this technology could affect online Violent Transnational Social Movements (VTSMs[1]) and their ability to spread extremist rhetoric and content that glorify terroristic violence such as mass shootings. Although research has shown that there is a link between the Internet and radicalization trajectories for extremists that fall within traditionally ideological categories, radicalization in these subcultural spaces and networks appears to place more emphasis on a fatalistic ideology known as ideological nihilism (Purdue, 2022). Ideological nihilism is shaped by apocalyptic thinking that involves personal grievances, disconnection and discontent with the broader society, and a fascination with aesthetic content surrounding the mass shooter persona (Purdue, 2022; Yousef, 2022). In extreme subcultures, this form of rebellion can lead to the encouragement of mass shootings (Purdue, 2022). Regarding the Highland Park mass shooting, for instance, Emmi Conley, an independent researcher for far-right movements, digital propaganda, and online subcultures, found through a digital footprint analysis of the shooter, Robert Crimo, that he did not express any ideological views whatsoever and that much of his radicalization occurred because of involvement in fringe subcultural spaces of the internet (Yousef, 2022). Much of his time was spent bonding with like-minded individuals and creating and sharing content that idealized terrorism and the Columbine shooters. This pattern of online radicalization has also been seen in the recent mass shootings in Buffalo and Uvalde, where one of the shooters frequented violent subcultural forums such as 4chan and 8chan which provided justification for violence using memes, dark humour, and literature that was misogynistic and white supremacist in nature, while the other shooter posted threats on social networking apps along with pictures of firearms. Sarah Hightower, an independent researcher of extreme far-

[1] See Kelshall et al. (2019), Growth of extremist echo chambers during lockdown periods: Ongoing concerns and implications in *DECODED: Understanding the post-covid-19 security landscape using structured models, approaches, and analytic techniques*, for more information on VTSMs and the consequences COVID-19 environment's isolating effect among VTSM members.

right movements and online cultic movements, states that this trajectory is not unique to one shooter and will likely be seen again in future shootings (Yousef, 2022).

This begs the question: does the blend of technologies making up the metaverse have the capacity to enhance the experience of radicalization due to its heightened realism and interoperable spaces, especially in a vulnerable segment such as the one described above? Some researchers would agree. Indeed, Elson et al. (2022) have found that the metaverse has increased potential in facilitating coordination, planning, and recruitment for terrorist acts; its immersive nature and the use of hyper-realistic avatars means that that extremist groups can recruit others in a greater capacity. Charismatic extremist leaders that have legitimacy and greater persuasive appeal can preach hateful rhetoric within decentralized virtual spaces that connect to other block chain spaces that users frequent. This virtually enhanced connectivity allows them to amplify their reach across networks, increasing the potential that their messages will resonate with future recruits. Based on the existing research surrounding VTSMs, online ideological nihilism, and features of the metaverse, it is highly likely that moving forward towards the metaverse one will see a parallel phenomenon of extremism exploiting decentralized subcultural spaces that are now 3D in presentation.

Based on the concerns outlined above, this article shall delve into several core aspects of the phenomenon relating to ideological nihilism within fringe online subcultures and their facilitation of mass shootings through isolated internet users who adopt VTSM beliefs and ideologies. First, the article provides a detailed description of the metaverse and what it has to offer in terms of strengthening tribal bonds with extremist networks. Second, it provides a conceptualized definition of mass shooting which is based on the nexus between violent extremism, terrorism, and online radicalization, as well as further insight into the development of mass shooter profiles as it applies to online fringe extremists. The final section will use the theory of malevolent creativity to examine how violent extremist culture in the metaverse is likely to take shape and proliferate, eventually culminating in the creation of a mass shooter.

The metaverse and Web3's effect on personal expression and creativity

Understanding the metaversal impact on online extremist culture-building demands an equal understanding of what Web3 will entail. At a practical level, Web3 is a *real-time, activity-based* Internet that will provide users immense autonomy in terms of personal expression and creativity in a permissionless and decentralized digital space. This will be enabled through three fundamental architectures, while being powered by Artificial Intelligence (AI) and machine learning (Melendez, 2022; Radoff, 2021a, 2021c). These are blockchains, Non-Fungible Tokens (NFTs), and smart contracts. All three of these architectures are integral to the foundation of the metaverse and its features and shall be discussed briefly.

Blockchains are based on Distributed Ledger Technology (DLT) and contain a string of records that are connected by cryptography and can be identified through time stamps, transaction dates, and cryptographic hash values that identify the previous block on the chain. The current focus of blockchain is through its use in facilitating cryptocurrency transactions without the use of a central authority. Although there has been much interest the past five years in cryptocurrency and its advantages in real-world investments, it is expected to be a prominent means for value exchange in the virtual economy of the metaverse (Draeger, 2015; Radoff, 2021b).

Directly related to blockchains are NFTs, which will be another prominent aspect of Web3 as well. Compared to cryptocurrency, which is fungible and can be broken down, NFTs are collectibles that are unique and indivisible. Furthermore, through their connection to a blockchain, NFTs allow an owner to have true ownership over it, providing them with knowledge of its history of transactions, level of scarcity, and programmability (Draeger, 2015).

Finally, another key architectural component will be smart contracts, which will allow efficient business processes to be conducted between parties without the need for an intermediary or broker. Like NFTs, programmability in smart contracts is also a key feature as encoded programming in the contract automatically allows it to activate when underlying conditions are met (Draeger, 2015; Radoff, 2021a). This means that users can remain confident that their transactions or agreements will be error-free and trust-less, meaning that they will not have to rely on agents to facilitate the process. Its applications will be beneficial in areas involving the Internet of Things, real estate, and escrow processes, to name a few. When combined with DLT, smart contracts will provide Decentralized Autonomous Organizations (DAOs) in the metaverse the means to automate their processes with the help from token holders affiliated with the entity that will act as management and vote on planning, operations, and strategy (Draeger, 2015; Reiff, 2022). In essence, smart contracts will be an efficient way to manage data without a centralized authority.

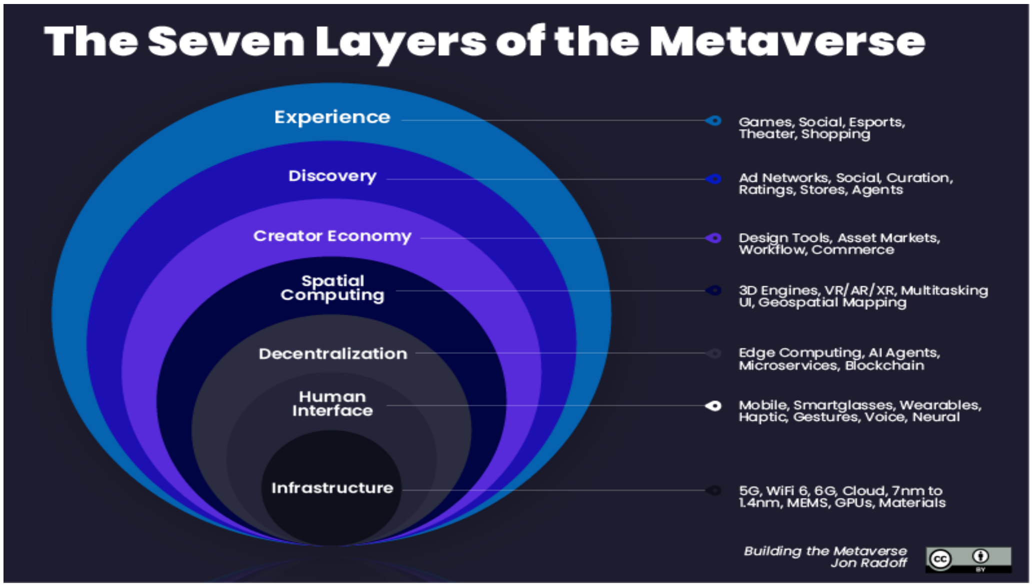
Overall, as a part of the prospect of a decentralized, interoperable, and permissionless online atmosphere, these three components will provide a solid foundation for the seven layers of the metaversal value-chain (Radoff, 2021b). In addition, the metaverse is expected to be a persistent, synchronous, and live experience for users with the added benefit of VR/AR/Mixed reality (XR) technology, providing an extremely social atmosphere as it bridges the physical and digital divide (Ball, 2020; Senno, 2022). What it is not, as Ball (2020) purports, is a virtual world, a game, or a digital economy alone. Instead, it is an expansive version of the Internet with its own set of protocols, technology, tubes, languages, content, and communicative devices on top of them. Its key value, however, will be in providing an *on-ramp experience* (Ball, 2020); wherein, social spaces will be populated by users and business competitors alike who will be able to create their own content and experiences that will intersect with one another, similarly to what is being seen currently in Fortnite, a game that contains elements of the metaverse. Such elements include the mashup of intellectual properties from competitors; a consistent identity that spans closed platforms; a gateway to a variety of social experiences; and finally, compensation for content that is created (Ball, 2020). Taken together, the three components along with the enhanced sociability provided by the on-ramp experience will likely be a worthwhile opportunity for online malign users, allowing them to fuel extremist-driven sentiments, radicalization, and violence justification in a greater capacity. How this is more likely to occur will be explained in the next section below.

Enhanced normalization of extremist culture within the metaverse

The potential security challenges of the metaverse stem from its seven-layer value chain (as seen in Figure 2 below) that enables users with greater creative freedom and experience without the need for gatekeepers and rent-takers, as seen through centralized platforms such as Facebook. Indeed, just as the metaverse holds tantalizing appeal to innovators, it will likely hold similar appeal to cybercriminals and extremists as well (Elson et al., 2022; Lloyd, 2021). As an unclassified report from Europol noted in 2017, the primary technologies and platforms that make up the seven-layer chain leaves the metaverse vulnerable to exploitation by cybercriminals who are known to "quickly adopt and integrate new technologies into their *modi operandi* or build brand-new business models around them" (Europol, 2017, as cited in Lloyd, 2021, para. 12). In terms of extremism, Elson et al. (2022) believe that the metaverse will allow terrorists and extremists expand their capacity for influence in essential areas such as recruitment, coordination, and targeting. For recruiting new recruits, VR would enable extremist leaders to entice new recruits by using hyper-realistic avatars of themselves to create virtual forums where they can present their radical views (Elson et al., 2022). VR companies such as Sensorium have already begun investing in the creation of realistic avatars that are driven by AI, making it likely that extremist networks online may end up using this to create numerous AI-driven avatars in their spaces (Takahashi, 2021). By programming them to espouse extremist rhetoric and providing them with significant capability for complex and unscripted conversations using natural language processing, young, impressionable users of the metaverse may be even more likely to become radicalized as they are exposed to a unique echo chamber in a metaversal environment (Canales, 2021; Melendez, 2022; Takahashi, 2021). In addition to the normalization of extremist culture, such recruitment tactics could streamline the process of radicalization, making it easier to influence vulnerable targets as AI-driven avatars in online metaverse spaces that are connected through interoperability beset them constantly.

Figure 2

The Seven Layers of the Metaverse


The Seven Layers of the Metaverse
Experience
Games, Social, Esports, Theater, Shopping
Discovery
Ad Networks, Social, Curation, Ratings, Stores, Agents
Creator Economy
Design Tools, Asset Markets, Workflow, Commerce
Spatial Computing
3D Engines, VR/AR/XR, Multitasking UI, Geospatial Mapping
Decentralization
Edge Computing, AI Agents, Microservices, Blockchain
Human Interface
Mobile, Smartglasses, Wearables, Haptic, Gestures, Voice, Neural
Infrastructure
5G, WiFi 6, 6G, Cloud, 7nm to 1.4nm, MEMS, GPUs, Materials
Building the Metaverse
Jon Radoff

Source: Radoff, 2021b

The use of online spaces by extremists has been a trending factor since the 1980s, when much online activity revolved around the creation of static webpages. As each iteration of the Internet has developed, extremist groups have leveraged novel technologies and platforms in recruiting, organizing, and coordinating online and offline activities. This has led to many services that were used by extremist groups to implement policies that would prevent their use of those services. However, this approach has been haphazard and reactionary and has not considered the tenacity of individuals who have found ways to circumvent their guidelines, such as using alternative and more permissive content-moderation platforms like Gab or Voat (Evans & Williams, 2022a). No doubt the pinnacle of this was the January 6, 2021, Capitol Hill Insurrection—an incident that was set apart from previous extremist incidents due to its sheer scale and success by organizers in inciting a mob towards real-world violence. As Byman (2021) notes, incendiary rhetoric by leaders can be magnified by those with large social media followings, which can likely predict higher incidences of violence as well as normalization of discourses that were previously considered taboo. Trump's rhetoric is an example of this because it created widespread shifts in sentiment towards extremism, which eventually shaped the direction of the violence that occurred. Thus, this is an exemplary indicator of how online tools by extremists can propel the creation of violent extremist culture.

To further understand how online immersion can fuel a violence glorified and hateful extremist culture in virtual communities, one must also understand the impact that anonymity has on online interactions. It is no coincidence that gaming platforms have been starkly linked to an uptick in extremist rhetoric involving different segments over the years. A major factor behind this has been anonymity. Anonymity has been linked to group identification processes that contribute to social bonding, which leads to developing an affinity for extremist beliefs (Evans & Williams, 2022b). An interview of eight former far-right extremists from Germany found that subversive online spaces that allow individuals to be anonymous leads to individuals using more aggressive language and issuing direct calls for action since there is less fear of social resistance or backlash (Koehler, 2014 as cited in Evans & Williams, 2022b). Suler (2004) refers to this effect as the *online disinhibition effect* and breaks it down into two dichotomous parts: benign disinhibition and toxic disinhibition. Benign disinhibition involves the desire to share one's secrets, fears, and wishes and aid another person, whereas toxic disinhibition involves using harsh language, anger, and threats to act out personal grievances. This combined effect is enhanced in environments that have one or more disinhibitory factors such as invisibility, dissociative anonymity, and individual personalities and differences because it allows the individual to take the initiative to seek out extreme communities and self-disclose aspects about themselves that they normally would not, and to a greater degree (Suler, 2004). In the context of gaming, however, factors such as solipsistic introjection, dissociative imagination, and the minimization of status and authority appear to be far more prevalent since the first two can enable the user to create a complex fantasy that markedly departs from their real-world persona, leading to the belief that any consequences involving their game-identity are separate from the demands and responsibilities of the real world (Suler, 2004). The minimization of status and authority in these environments may also fuel extremist rhetoric since users are usually driven by the belief that everyone is an equal on the Internet and that the growth of the Internet and development of new online spaces make them “innovative, independent-minded explorers and pioneers” (Suler, 2004, p. 324). This sense of freedom can facilitate the creation and maintenance of dark, violence-glorified subcultures that are devoid of any views that are ideologically disparate; thus, allowing for the strengthening of bonds and normalization of extremist discourse (Kelshall et al., 2020; Senno, 2022; Yousef, 2022). Furthermore, a subculture that is out of sync with the mainstream can create a sense of exclusion, leading to a polarized ‘us vs them’ mentality (Shurin, 2022). Overall, this philosophy along with the Internet architecture (message boards, alternative tech communication, social media, etc.) that provides anonymity can contribute to the creation of interpersonal dynamics that are centered around *other deindividuation* (or in-group/out-group classifications) processes that can fuel anger, which may manifest through the use of hateful humour, harassment, and other abusive behavior (Evans & Williams, 2022b; Schlegel, 2022a; Suler, 2004). In turn, the addictive properties associated with aggressive virtual behavior can reinforce identification with extremist groups, in-group belonging, and ideological hardening, leading to greater susceptibility to far-right propaganda (Evans & Williams, 2022b).

In the end, this may have massive implications for interactions in the metaverse, especially in the gaming sector where most investments in networks and graphics technologies have taken place and is essentially the “heart of the metaverse” (Lloyd, 2021, para. 14). Senno (2022) notes that the cross-border nature of cyberspace and emerging online spaces facilitated by complex technologies that allow for anonymity and non-traceability will inevitably create a breakdown in the ability to regulate, leading to freedom of action towards crime. Both the creator economy and gaming sector of the metaverse are likely to be targets of opportunistic criminals looking to launder illicit proceeds, which, in some cases, this has been in the form of blockchain-based assets such as NFTs (Lloyd, 2021). NFTs are likely to become a favoured medium of exchange for criminal activities due to its profit potential, lack of regulation, and difficulty in tracing and monitoring (Lloyd, 2021; Pely, 2022). The digital art trade is an example of this and is likely to accentuate money laundering as digital art NFTs are used to hide and disguise illicit funds through peer-to-peer transactions (Arasingham & Goodman, 2022). Overall, it is apparent that NFTs, along with cryptocurrencies, will be a significant factor that drives extremists towards the gaming sector.

With this in mind, the gaming sector in the metaverse will be increasingly vulnerable to facilitating extremist activity and radicalization. Its lack of supervision, persistence of anonymity, and ability to provide combat training is likely to pave the way for the shaping of extremist culture in the metaverse as extremist leaders attempt to expand “support for extremist narratives through immersive experiential modes that are powerful and difficult to crush” (Senno, 2022, para. 34). The Buffalo shooter, Peyton Gendron, who carried out the racially motivated murders of 10 people in a supermarket, spent months leaving a digital footprint of his messages over Discord, an online real-time chat platform that was initially used by gamers to communicate but is now used as an all-purpose tool that hosts various communities (Chayka, 2022). The platform separates itself from the algorithmic feeding of extremist content (seen over sites such as Facebook and Twitter) and, instead, allows users to create their own communities of influencers that can draw passive consumers into their orbit, similar to what Gendron did, consciously aware that his messages might encourage others to follow in his tracks (Chayka, 2022). Twitch, another platform with gaming origins, was also used to broadcast a livestream of the mass shooting in real-time. The reliance on these platforms suggests that there are favourable features for violent extremists that differ from those offered by big data platforms such as Facebook (Hadley, 2021). In the case of the Buffalo shooter, the ability to privatize his Discord community on an ‘invite-only’ basis and willingness to use the real-time feature of Twitch at the exact moment of the shooting significantly increased his success in evading detection by platform moderators. These moderators only became aware and acted in the aftermath of the incident, just as in the Christchurch shooting (Chayka, 2022; Holmes, 2019). Based on this, it is apparent that weak supervision and regulation due to decentralization, anonymity, and real-time features (Radoff, 2021b) of online platforms will play an integral role in facilitating extremism and radicalization in the metaverse as time goes on.

Lastly, the ability to train for terrorist scenarios using VR/AR will be a unique aspect for prospective violent extremists. While the connection between video games and violence has always been tenuous at best, even during the backlash of the 1990s, research still shows that violent video games are associated with lower empathy, a desensitization to violence on both the neural and the behavioural level, and the reduction of cognitive and emotional responses to violent stimuli (Schlegel, 2020b; Senno, 2022). The lack of empathy and desensitization can be facilitated by in-game moral disengagement processes that selectively deactivate moral control mechanisms; thereby, contributing to the acceptance and exercise of violence to a greater degree (Bandura, 1990; & Hartman, 2014 as cited in Schlegel, 2020b).

In addition, it may also contribute to a perceived self-efficacy or the ability to produce a desired outcome. The immersive and interactive nature of video games can promote greater identification with one's avatar causing them to feel more aggression, which can translate to a desire to fulfill violent extremist aggression if shaped by extremist communities (Schlegel, 2020b). Virtual worlds can facilitate this self-efficacy towards a malevolent outcome, as Cole (2012) found when examining a virtual world called Second Life from the extremist perspective, using an avatar that was exposed to graphic content of radical Islamic propaganda. He concluded that the level of immersion experienced through "continuous auditory and visual stimuli can cause a person to self-identify with an extremist group's views" (Cole, 2012, p. 78). This has been confirmed in some studies that have found a correlation with violent gameplay and cognitive aggression, particularly in an environment with greater presence or immersion (American Psychological Association [APA], 2020; Anderson et al., 2010; Lull & Bushman, 2016). On the other hand, other studies show that the link between violent VR video games and aggression (cognition and behavior) is inconclusive (Drummond et al., 2021; Ferguson et al., 2021). However, as Haam and Spaaj (2015) have determined, the pathway to violent extremism is multifaceted, and it involves conveying personal and political grievances to supportive online networks and being enabled by charismatic extremists; therefore, these studies may not be viable in the context of the metaverse and its features.

Conceptualizing a mass shooting as it relates to influential spaces in the metaverse

To conceptualize mass shootings for the purposes of this article, it is necessary to look at past literature that has attempted to define a mass shooting event. Historically, studies have struggled to develop a uniform definition for mass shooting that differs from terrorism, as no legal definition for a mass shooting has ever been established. Furthermore, most definitions have been contradictory and inconsistent due to either conflating terrorist incidents with mass shooting incidents or having these incidents separate from the analysis, which can make it difficult to assess how often such incidents have occurred and whether there is an uptrend or downtrend. (Booty et al., 2019; Lopez et al., 2020; Smart & Schell, 2021). Generally, however, the definition has typically comprised characteristic elements such as the casualty threshold and the contextual distinction between different types of mass shootings. Both of these aspects are controversial. Regarding the casualty threshold, which is usually set to four or more fatalities, excluding the shooter, this approach is controversial because it does not consider the number of injured that may exceed the fatalities (Booty et al., 2019; Smart &

Schell, 2021). The contextual disagreement on the definition arises because it may or may not include mass shootings that occur from criminal gang activity or domestic violence into the data for public mass shootings, which can inflate/deflate the number of mass shooting incidents counted (Smart & Schell, 2021). As Krouse & Richardson (2015) found, combining counts of different contexts, such as familicide and felony, with public mass shootings can lead to erroneous generalizations that can lead to errors in implementing preventative measures. They also found in their analysis on mass shootings that over a 15-year period (1998-2013), there were only 4.4 mass shootings per year on average compared to the relatively greater frequencies involving familicide and felony mass shootings, which demonstrates the rarity of mass shootings (Booty et al., 2019). Overall, the inconsistencies in definitional aspects, along with the rare nature of mass shootings, have been significant issues for researchers in their assessments of mass shootings.

Besides the lack of a uniform and meaningful definition and consistent data sources, another major fact that often seems to be missing from databases is the intent of the mass shooter, which is necessary in ascertaining the ideological disposition of the shooter (Lopez et al., 2020). In terms of the conceptual distinction between violent extremism and terrorism, the diversity in definitions tends to suggest that violent extremism has broader connotations, dealing with an array of different types of ideologically motivated violence that fall short of terrorism (United Nations Office on Drugs and Crime [UNODC], 2018). In Canada, it is defined as an offence that is “primarily motivated by extreme political, religious or ideological views” (UNODC, 2018, para. 18). It can also be broken down into several categories, one of which is Ideologically Motivated Violent Extremism (IMVE). IMVE consists of ideals and grievances based on a variety of ideologies and centers on having a personal narrative informed by different sources, including dark online subcultural spaces (Canadian Security Intelligence Service, 2019). These definitions will be significant to the conceptualization of a mass shooting definition because of the different IMVE segments that past violent extremists have alluded to prior to their attacks.

Based on what has been discussed above about IMVE and the tendency of fringe online spaces to increase radicalization by supporting narratives that promote and glorify mass violence and past extremists, public mass shootings can be considered acts of terrorism. Using four basic criteria from standard, domestic and international definitions of terrorism, Hunter et al. (2020) conducted an analysis of 105 mass shooting incidents that occurred from 1982 to 2018 in the U.S. They discovered that 82% of the incidents closely matched the criteria utilized. The criteria include: a political, religious, ideological, or social motivation; intent to reach a larger audience; the motivation not involving personal monetary gain; and the manifestation of an ‘enemy/other.’ Using these criteria as the basis, in conjunction with what has been discussed in the previous section, public mass shootings can be conceptualized as: *ideologically motivated violent extremist incidents, in which four or more individuals have been killed or injured by firearms in locations that are near one another, and by desensitized individuals with personal grievances who are motivated by support from extreme, violence-oriented, and ideologically segmented online subcultures.*

Malevolent creativity and the creation of a ‘mass shooter culture’

The spatial computing aspect of the metaverse will greatly accelerate the level of creativity shown by users as creator-driven experiences are heightened using integrated tooling, discovery, social networking, and a world monetization functions. The decentralized and open nature of the metaverse, as well as its convergence through internet technologies and Extended Reality (XR), will provide extremists with malevolent, creative ways to conduct their activities without the constraints and limitations of centralized platforms that limit their autonomy. Elson et al., (2022) believe that recruitment attempts in the metaverse could involve using deep fake technology to recreate past violent extremists that could appeal to newer recruits. They could also use innovative ways to coordinate in the metaverse as they train for terrorist attack scenarios using virtual representations of real buildings; AR objects such as virtual arrows could even aid violent extremists in guiding them and helping identify targets. Finally, the method of attacking virtual targets may help violent extremists achieve their objective of creating widespread fear and psychological harm in the real world, even putting business owners at risk of financial loss (Elson et al, 2022). These are some of the ways extremists may benefit from the metaverse.

The theory of malevolent creativity ties into what Elson et al. (2022) have stated above. Originally developed by Cropley et al. (2008), the malevolent creativity model stresses a dark side to creativity, asserting that certain groups use creativity to fulfill their aims towards conducting acts that have intentionally harmful consequences for another group. In addition, the model holds that creative terror products by groups eventually decay in the novelty they exhibit, similar to the 9/11 attacks in which once the passengers of the United 93 flight knew what was going on, they were able to overcome their hijackers. This idea can also be applied towards public mass shootings that are subject to the contagion effect and trigger further shootings by other shooters who become inspired by the aftermath of the preceding one (Keierleber, 2022). In a centralized environment, law enforcement officials and content moderators are able to heighten their scrutiny towards online content that indicates an impending shooting; thus, reducing the novelty of the mass shooting that took place recently. However, in a metaversal environment, the novelty would remain constant due to decentralization-enabled permissionless, trustless, and private spaces that extremists would be able to operate from which would prevent exposure of any content (text or images in the form of NFTs) that would insinuate another impending shooting. This model thus shows that there is ample opportunity for the metaverse to aid disgruntled extremists in facilitating terror products in the form of mass shootings.

Another closely linked concept is malevolent innovation. This is essentially the act of manifesting one's ideation of a malevolent creative idea that involves intentional harm, such as the act of committing a mass public shooting (Hunter et al., 2021). As reiterated earlier, online gaming that utilizes VR/AR is likely to act as a platform for combat training; the greater the immersion, the more likely an individual will develop real-world functional skill sets necessary to carry out successfully an act of firearms-related terrorism. The changes in one's brain network can facilitate the development of sensorimotor skills that enhance reflexes used for shooting, which is essentially what the U.S. Army focuses on when training recruits for combat proficiency in their Synthetic Training Environment (STE) (Adamovich, 2009; Rozman, 2020). As Adamovich (2009) notes, confirming Lull and Bushman's (2016) conclusion, "the fidelity of the VR environment may be an important factor in its effectiveness to recruit neural circuits and deliver desirable outcomes at the functional level" (p. 31-32). Thus, this shows the efficacy of metaverse-driven gaming in allowing extremists to move from malevolent creativity towards innovation.

Conclusion

In essence, the metaverse holds vast potential in many different areas. However, history has shown that extremists will always look towards novel methods of carrying out their activities, whether these are recruitment, fundraising, or even violent acts. Moreover, the trend in isolated males who are prone to the rhetoric of dark subcultures online raises many questions on the social processes affiliated with the facilitation of online radicalization and mobilization towards mass casualty attacks. Rather than accentuating traditional ideologies, many past violent extremists, such as the Buffalo and Highland Park shooters, have displayed an amalgamation of different extremist ideologies in their writings. The online spaces they affiliated with allowed them to engage in a normalization of extremist language that involved right wing, misogynistic, and anti-government segments. At the same time, the discussions involved a sense of nihilism due to the gamified language being used which made references to elements of gaming (i.e., points, leaderboards, kill ratio, and badges) in non-gaming contexts, likely for the purposes of contributing to behavioral change (Schlegel, 2020b). The manifesto written by the Buffalo shooter and the animated videos created by the Highland Park shooter also suggested a fascination with previous mass shooters and firearms in general. Considering that the metaverse's decentralization and creator autonomy will make it difficult to track these discussions, much work needs to be done in determining what methods are useful in deterring and detecting extremist literature and communications in the metaverse.

Furthermore, it is necessary to note the similarities and distinctions between extremist radicalization that would occur in the metaverse and online radicalization that is currently taking place over Web 2.0, which involves internet forums, chat sites/apps, and major social media platforms. For instance, virtual actions, such as attacking avatars through soft and kinetic means, and virtual representations of significant landmarks/institutions would provide one way for radicals to bond with other like-minded users. This would be no different from how they bond on Web 2.0—through the sharing of memes, vulgar misogynistic/racist posts, and humour; antisemitic conspiracy theories about replacement; and glorification of violence, particularly mass shootings, through aesthetic media (videos and images that glorify past mass shooters). Conversely, however, it is different from other forms of radicalization in the sense that the nihilist sentiment conveyed in these spaces, that is, the desensitization towards death and violence, is the critical element that separates those who commit mass shootings from other online radicals that do not. The latter may instead choose to either sympathize with them or goad them into carrying out the act, while contributing to the extremist echo chamber in other ways via the online disinhibition effect.

In addition to this juxtaposition, it should be recognized that the gaming industry has invested the most in the metaverse with their technologies revolving around the use of VR, AR, and XR. The heightened capacity for immersion has an immense potential for taking video game radicalization to another level, especially in lieu of research involving its ability to trigger cognitive aggression in individuals, as well as recent applications towards military combat training. More research must be done on whether there is a true link between aggressive behavior that translates to extreme violence and immersive gaming technology.

Finally, the model of malevolent creativity along with its close counterpart, malevolent innovation, show significant potential in assessing how the metaverse may contribute to violent extremist ideation which falls in line with malevolent creativity. More research must be done, however, in determining how the metaverse can influence an individual to acquire other skills that would allow them to successfully carry out an act of violence.

References

Adamovich, V. S., Fluet, G. G., Tunik, E., & Merians, S. A. (2009). Sensorimotor training in virtual reality: A review. *Neurorehabilitation,* (25), 29-44. https://doi.org/10.3233/NRE-2009-0497

American Psychological Association. (2020). *APA resolution on violent video games: February 2020 revision to the 2015 resolution.* https://www.apa.org/about/policy/resolution-violent-video-games.pdf

Anderson, A. C., Ihori, N., Shibuya, A., Bushman, J. B., Swing, L. E., Sakamoto, A., Rothstein, R. H., & Saleem, M. (2010). Violent video game effects on aggression, empathy, and prosocial behavior in eastern and western countries: A meta-analytic review. *Psychological Bulletin, 136*(2), 151-173. https://doi.org/10.1037/a0018251

Arasingham, A., & Goodman, P. M. (2022, February 10). *Insights from the U.S. Treasury Department's study of the global art trade*. CSIS: Center for Strategic & International Studies. https://www.csis.org/analysis/insights-us-treasury-departments-study-global-art-trade

Ball, M. (2020, January 13). *The metaverse: What it is, where to find it, and who will build it.* MatthewBal.vcl. https://www.matthewball.vc/all/themetaverse

Bandura, A. (1990). Selective Activation and Disengagement of Moral Control. *Journal of Social Issues,* 46(1), 27-46. https://doi.org/10.1111/j.1540-4560.1990.tb00270.x

Booty, M., O'Dwyer, J., Webster, D., McCourt, A., & Crifasi, C. (2019). Describing a "mass shooting": The role of databases in understanding burden. *Injury Epidemiology, 6*(47), 1-8. https://doi.org/10.1186/s40621-019-0226-7

Byman, D. (2021, April 9). *How hateful rhetoric connects to real-world violence.* The Brookings Institution. https://www.brookings.edu/blog/order-from-chaos/2021/04/09/how-hateful-rhetoric-connects-to-real-world-violence/

Canadian Security Intelligence Service. (2019). *Threats to the security of Canada and Canadian interests. CSIS Public Report 2019.* Government of Canada. https://www.canada.ca/en/security-intelligence-service/corporate/publications/2019-public-report/threats-to-the-security-of-canada-and-canadian-interests.html

Canales, K. (2021, November 20). Mark Zuckerberg's metaverse could fracture the world as we know it – letting people 'reality block' things that they disagree with and making polarization even worse. *Business Insider*. https://www.businessinsider.com/facebook-meta-metaverse-splinter-reality-more-2021-11

Chayka, K. (2022, May 19). The online spaces that enable mass shooters. *The New Yorker*. https://www.newyorker.com/culture/infinite-scroll/the-online-spaces-that-enable-mass-shooters

Cole, J. (2012). Radicalisation in virtual worlds: Second Life through the eyes of an avatar. *Journal of Policing, Intelligence, and Counter Terrorism, 7*(1), 66-79. http://dx.doi.org/10.1080/18335330.2012.653197

Cropley, H. D., Kaufman, C. J., & Cropley, J. A. (2008). Malevolent creativity: A functional model of creativity in terrorism and crime. *Creativity Research Journal, 20*(2), 105-115. https://doi.org/10.1080/10400410802059424

Draeger, D. D. (2015). *More than money: Get the gist on bitcoins, blockchains, and smart contracts.* Department of Justice. Government of Canada. https://publications.gc.ca/site/eng/9.870208/publication.html

Drummond, A., Sauer, D.J., Ferguson, J.C., Cannon, R.P., & Hall, C.L. (2021). Violent and non-violent virtual reality video games: Influences on affect, aggressive cognition, and aggressive behavior. Two pre-registered experiments. *Journal of Experimental Social Psychology, 95,* 1-9. https://doi.org/10.1016/j.jesp.2021.104119

Elson, S. J., Doctor, C. A., & Hunter, S. (2022, January 7). *The metaverse offers a future full of potential – for terrorists and extremists too.* The Conversation. https://theconversation.com/the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too-173622

Evans, T. A. & Williams, J. H. (2022a*). Extremist use of online spaces*. RAND Corporation. https://doi.org/10.7249/CTA1458-1

Evans, T. A. & Williams, J. H. (2022b*). How extremism operates online: A primer*. RAND Corporation. https://doi.org/10.7249/PEA1458-2

Ferguson, J. C., Gryshyna, A., Kim, J.S., Knowles, E., Nadeem, Z., Cardozo, I., Esser, C., Trebbi, V., & Willis, E. (2021). Video games, frustration, violence, and virtual reality: two studies. *British Journal of Social Psychology, 61*(1), 83-99. https://doi.org/10.1111/bjso.12471

Haam, M. & Spaaj, R. (2015). *Lone wolf terrorism in America: Using knowledge of radicalization pathways to forge prevention strategies*. Indiana State University. https://www.ojp.gov/pdffiles1/nij/grants/248691.pdf

Hadley, A. (2021, May 31). *Terrorists are hiding where they can't be moderated.* Wired. https://www.wired.co.uk/article/terrorists-dweb

Hartmann, T., Krakowiak, K.M., & Tsay-Vogel, M. (2014). How violent video games communicate violence: A literature review and content analysis of moral disengagement factors. *Communication Monographs, 81*(3), 310-332. https://doi.org/10.1080/03637751.2014.922206

Hunter, Y. L., Ginn, H. M., Storyllewellyn, S., & Rutland, J. (2020). Are mass shootings acts of terror? Applying key criteria in definitions of terrorism to mass shootings in the United States from 1982 to 2018. *Behavioral Sciences of Terrorism and Political Aggression*, *13*(4), 265-294. https://doi.org/10.1080/19434472.2020.1762108

Hunter, T. S., Miller, R. S., & Walters, K. (2021). Malevolent creativity and malevolent innovation: a critical but tenuous linkage. *Creativity Research Journal*, *34*(2), 123-144. https://doi.org/10.1080/10400419.2021.1987735

Keierleber, M. (2022, May 25). *The contagion effect: From Buffalo to Uvalde, 16 mass shootings in just 10 days.* The74. https://www.the74million.org/article/the-contagion-effect-from-buffalo-to-uvalde-16-mass-shootings-in-just-10-days/

Kelshall, M. C., Franco, E., Kale, A. (2019). Impact of violent transnational social movements on a post-covid environment. In Kelshall, M. C., Archutowski, N., & Meyers, S. (Eds.), *DECODED: Understanding the post-COVID-19 security landscape using structured models, approaches, and analytic techniques* (pp. 79-93). Canadian Association of Security and Intelligence Studies-Vancouver. https://casisvancouver.ca/wp-content/uploads/2020/08/DECODED-2020.08.21-WEB.pdf

Koehler, D. (2014). The radical online: Individual radicalization processes and the role of the internet. *Journal for Deradicalization, 1,* 116–134. https://journals.sfu.ca/jd/index.php/jd/article/view/8

Krouse, J. W. & Richardson, J. D. (2015, July 30). *Mass murder with firearms: Incidents and victims, 1999-2013.* Congressional Research Service. https://sgp.fas.org/crs/misc/R44126.pdf

Lloyd, T. (2021, November 29). Facebook's metaverse heralds a brave new underworld of metacrime. *The New Republic.* https://newrepublic.com/article/164497/facebook-metaverse-cybercrime-marc-zuckerberg

Lopez, E. B., Crimmins, M. D., & Haskins, A. P. (2020). Advancing mass shooting research to inform practice. *National Institute of Justice.* https://www.ojp.gov/pdffiles1/nij/254469.pdf

Lull, B. R. & Bushman, J. B. (2016). Immersed in violence: Presence mediates the effect of 3D violent video gameplay on angry feelings. *Psychology of Popular Media Culture, 5*(2), 133-144. https://doi.org/10.1037/ppm0000062

Melendez, C. (2022, April 18). The metaverse: Driven by AI, along with the old fashioned kind of intelligence. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2022/04/18/the-metaverse-driven-by-ai-along-with-the-old-fashioned-kind-of-intelligence/?sh=6d9fa23f1b36

Pely, D. (2022, January 17). *The dark side of the metaverse.* USC Price: Safe Communities Institute. https://sci.usc.edu/2022/01/17/the-dark-side-of-the-metaverse/

Purdue, S. (2022, July 13). *Ideological nihilism and aesthetic violence: Mass shooters and online antisocial subcultures*. Global Network on Extremism and Technology. https://gnet-research.org/2022/07/13/ideological-nihilism-and-aesthetic-violence-mass-shooters-and-online-antisocial-subcultures/

Radoff, J. (2021a, May 19). *9 megatrends shaping the metaverse*. Medium. https://medium.com/building-the-metaverse/9-megatrends-shaping-the-metaverse-93b91c159375

Radoff, J. (2021b, April 7). *The Metaverse value-chain*. Medium. https://medium.com/building-the-metaverse/the-metaverse-value-chain-afcf9e09e3a7

Radoff, J. (2021c, November 22). *Web3, interoperability, and the Metaverse*. Medium. https://medium.com/building-the-metaverse/web3-interoperability-and-the-metaverse-5b252dc39da

Reiff, N. (2022, July 11). *Decentralized Autonomous Organizations (DAO): Definition, purpose, and example*. Investopedia. https://www.investopedia.com/tech/what-dao/

Rozman, J. (2020). *The Synthetic Training Environment.* The Association of the United States Army. https://www.ausa.org/sites/default/files/publications/SL-20-6-The-Synthetic-Training-Environment.pdf

Schlegel, L. (2020a, April 13). How video games could facilitate radicalization processes. *Regional Cooperation Council*. https://www.rcc.int/swp/news/278/how-video-games-could-facilitate-radicalization-processes

Schlegel, L. (2020b). Jumanji extremism? How games and gamification could facilitate radicalization processes. *Journal for Deradicalization,* (23), 1-44. https://journals.sfu.ca/jd/index.php/jd/article/view/359

Senno, S. (2022, April 26). *The metaverse, an opportunity for society, or terrorism? Challenges in the field of prevention*. AMIStaDeS – Study Centre for the Promotion of International Culture. https://en.amistades.info/post/metaverse-an-opportunity-for-society-or-terrorism

Shurin, J. (2022, January 26). *The latest frontier in radicalization: Gaming*. CARR: Center for Analysis of the Radical Right. https://www.radicalrightanalysis.com/2022/01/26/the-latest-frontier-in-radicalization-gaming/

Smart, R. & Schell, L. T. (2021, April 15). *Mass shootings in the United States*. RAND Corporation. https://www.rand.org/research/gun-policy/analysis/essays/mass-shootings.html

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior, 7*(3), 321-326. https://doi.org/10.1089/1094931041291295

Takahashi, D. (2021, August 4). *Sensorium demos AI-driven avatars as latest virtual beings.* Venture Beat. https://venturebeat.com/games/sensorium-demos-ai-driven-avatars-as-latest-virtual-beings/

United Nations Office of Drugs and Crime. (2018, July). *'Radicalization' and 'Violent Extremism'.* University Module Series: Counter-Terrorism. https://www.unodc.org/e4j/zh/terrorism/module-2/key-issues/radicalization-violent-extremism.html

Vandhana, N. (2022, March). *Why entrepreneurs will dominate metaverse technology?* Futurism. https://vocal.media/futurism/why-entrepreneurs-will-dominate-metaverse-technology

Yousef, O. (2022, July 6). *Why the Highland Park suspect represents a different kind of violent extremism*. NPR. https://www.npr.org/2022/07/06/1110013040/the-highland-park-suspect-breaks-the-mold-on-violent-extremists

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/