Ready Player Bad: The Future Rise of Extremism and Terrorism in the Metaverse

A.Procopiou
School of Sciences University of Central Lancashire, Cyprus Larnaca, Cyprus a.procopiou@uclan.ac.uk

***Abstract*—In the not so distant future, the rise of the metaverse will bring multiple opportunities to people and societies all over the world. Through pioneering technologies integrated, it aims to revolutionise and significantly improve our lives. Unfortunately the metaverse can also be exploited and abused to facilitate the operations of extremists and terrorists as it has already happened in social media and online blogs and forums. Using the metaverse's virtual reality, A.I., digital twins and avatars to their advantage, the various extremist/terrorist organisations and groups can successfully spread their radical ideologies and propaganda, recruit new members and plan their attacks more effectively and with minimum costs. In the metaverse, such operations will have greater impact since the users will be an actual part of the metaverse and therefore fully immersed in it. In this paper, we aim to provide a better understanding of how extremists and terrorists can exploit the metaverse and its services through the usage of appropriate discussion and relevant examples. Concluding, we give some general direction on what needs to be done to prevent such unfortunate scenarios.**

***Index Terms*—Metaverse, extremism, terrorism, social media, safety, security, counter-extremism/terrorism, virtual reality**

I. Introduction

Metaverse, a combination of the words "meta" (transcending) and "universe" firstly mentioned by [1], is perhaps the most pioneering asset of Internet 3.0. It denotes the integration of highly detailed and fully interactive three-dimensional (3D) virtual worlds which can be accessed by humans through the usage of avatars. Avatars can interact with each other, with applications and services the metaverse provides as well with both the physical and virtual environments. Previous attempts to create the metaverse occured in the past such as Second Life, Fortnite, Roblox and VRChat [3]. However, it has only recently started becoming increasingly popular and attracted the interest of big technological corporations such as Microsoft, Meta (previously Facebook), Google and Apple [4]. The opportunities are endless and appealing. Examples include connecting the world through immersive experience to its users with more meaningful interactions [5], providing an efficient online shopping experience [6], enabling online learning and education environments [7], and new opportunities for financial gain [8]. However, there is likely to be a dark side of the metaverse. Internet 2.0, mainly through social media, enabled the conduction of criminal acts in cyberspace such as cybercrime [9], cyberbullying, online hate and discrimination [10]. One of the most dangerous consequences was the emergence of online extremist/terrorist acts, including online propaganda, radicalisation, recruitment of new members globally and planning and coordination of attacks [11], [12].

Currently, extremist/terrorist organisations thrive in social media platforms such as Twitter, Facebook, YouTube and discussion forums such as Reddit and 4chan [13]. With the rise of the metaverse, the impact will be magnified since users will be fully immersed though the various technologies. Hence, users will be involved in fully interactive experiences with their senses as possible, but also have their senses stimulated. Unfortunately, through this immersive experience, users are therefore more vulnerable to the extremists' and terrorists' recruitment approaches, propaganda and radicalisation methods. Therefore, it is only a matter of time before the various extremist/terrorist groups move their operations to the metaverse. In this paper, we discuss how extremists/terrorists could violate and exploit the metaverse and its properties. By providing appropriate examples, we explain how the different extremist/terrorist organisations could successfully accomplish their operations in the metaverse. Proceeding, we conclude on what future directions could be taken to respond and eventually prevent such acts.

II. Background Knowledge

A. Metavserse Technologies

1) Virtual Reality (VR): VR denotes the simulated experience in fully virtual environments [14]. Virtual environments can exhibit similarities to the real world or be completely different [15]. In a virtual environment, users can create their own personal content such as street art, interact with other users and participate in collaborative activities in real-time.

2) Augmented Reality (AR): AR enhances the physical world by alternating its surroundings. Using different information channels, such as audio, visuals, smell and touch, and haptics [16] all virtual content can be successfully presented to the users with which they can fully interact.

3) Digital Twins (DT) and the Internet of Things (IoT): DT are a virtual replication of a physical object or a real-world, that aims to help in better and more efficient simulation, integration and monitoring. IoT sensors deployed in the real world, monitor the physical counterpart of the digital twin and send the acquired data. Upon receiving the data, the digital twin simulates the physical object/entity in real time [17].

B. Avatars

In the metaverse, an avatar is the digital representation of a human [18]. This representation includes the user's overall behaviour and interaction with other users [19] and

the integration of their own gestures, facial expressions and movements [15].

C. Extremism and Terrorism Important Concepts

Extremism and terrorism are two complex phenomena rather than two distinct concepts. The idea of what is considered extremism and terrorism can change based on the geographical location, culture, customs, social norms, religion, and political affairs. However, in this paper we give a brief explanation on what we define as extremism and terrorism as well as important associated concepts.

Ideology: Defined as the way of thinking, content, behaviour of an individual, a group or culture [20]. Usually applied to political and religious context, but can also correspond to general ideas, customs and beliefs.

Extremism: Encompasses all the supporting beliefs, ideas, ways of thinking and acting that are extreme from the general public [21]. Extremism can be religious, political or of any other belief-based type.

Terrorism: The use of violent and fearful means to forcefully achieve an ideological aim. Mainly describes all international violent acts during a time of peace or during war against unarmed individuals and groups (e.g. civilians) [22].

Propaganda: Includes all the information classified as biased and inaccurate, usually used to justify a radical point of view and acts [23]. Propaganda can be conducted for political, religious or other types of ideology reasons.

Radicalisation: Denotes the radical changes in ideas, beliefs, thought processes, feelings and emotions and overall behaviour towards the extreme domain. This change is often accompanied by actively promoting violence and sacrifice [24]. Unlike propaganda which tries to mislead individuals, online radicalisation mainly aims to mislead individuals by exploiting and manipulating their beliefs, opinions, emotions, feelings, and experiences.

Recruitment: Encompasses all the relevant actions towards persuading people (most likely young individuals) to join and often sacrifice for the extremist or terrorist group [25]. Recruitment in cyberspace mainly occurs through social media and forums. Extremists and terrorists mainly rely on text, images, videos and music to communicate their agenda and recruit individuals.

III. Extremism and Terrorism in the Metaverse Concerns and Discussion

A. Propaganda, Radicalisation and Recruitment

Propaganda and radicalisation through social media proved significantly effective as they are easily reachable to the masses regardless of their geographical locations. Instead of people having to physically attend a gathering to interact with the source of propaganda, they were able to watch videos on video-streaming platforms, read online articles through micro-blogging/blogging platforms, or go through a series of posts which could include various types of media such as short video-clips, images, text and sound-clips [21]. Unfortunately, in the metaverse people are in danger of being fully immersed to extremist/terrorist propaganda, radicalisation and recruitment. Through virtual and/or augmented reality, extremist and terrorist organisations will be able to create their own metaverse-esque spaces [26], [28]. Hence, through the virtual spaces, a shared sense of space and time is achieved between old and new members of the extremist or terrorist organisation.

Also, using the content creation services the metaverse offers, these virtual spaces will be transformed in places where extremist/terrorist ideologies thrive through the usage of radicalised content and propaganda such as posters, street wall graffiti, flags and banners, and video/sound recordings speeches from avatars of important figures (either alive or deceased). Using them, these organisations will be free to express their extremist and terrorist ideology, spread their propaganda, recruit new members in the organisations and radicalise new and existing members. Such places are likely to be the meeting points of the organisation's members where they are free to consistently interact with each other in real-time [15]. They will be able to talk to each other, exchange views about their engagement with other relevant organisations, hold meetings and speeches, and plan their future recruitment actions.

In more detail, through virtual and/or augmented reality, people will be able to "virtually fully attend" a speech by the extremist/terrorist organisation and directly interact with its members. Instead of just live-streaming a speech, watching videos or interacting with members of the extremist or terrorist organisation through chat rooms and forums, individuals will now have the opportunity to directly engage with them in the metaverse and emotionally connect with them on a personal level [27], [28]. Therefore, potential new members and newly recruited ones will immediately feel part of the community and are likely to gain more responsibilities with regards to the organisation's activities and actions.

Furthermore, with the usage of VR/AR and A.I., important past figures of the extremist or terrorist ideologies such as Adolf Hitler or Osama Bin Laden could be brought back to life [27], [28], [29]. Their presence will not only attract new members but also provide additional benefits to the organisation. Firstly, it will create a sense of self-duty and self-importance between the members as potentially the founding member, or one of the founding members, is "alive" and directly speaking to them, urging them to "do what is right" or "save the world from evil". In addition, it will create a sense of unity, as their "leader" is "alive" and ready to inspire and guide them. Therefore, members of the organisation are significantly radicalised and it is potentially easier to recruit new members as the presence of a founding figure will most likely be catalytic in them joining the organisation. In addition, through the usage of avatars, extremists and terrorists will be able to directly affect potential new members and newly recruited ones on an emotional level. The avatars' highly detailed design and appearance, including the detailed face and body, subtle and minor expressions, fidelity, the details in the avatar's gestures and spatial positions, the design of avatar behaviours, and the synchronisation of the avatar's body movements can have a significant psychological impact [15].

In detail, through the characteristics mentioned, the extremists and terrorists can create a sense of fear and authority that can influence the new members into engaging in highly criminal acts even when having doubts.

Through digital twins, people will virtually interact with important artifacts of extremist and terrorist organisations. An example includes badges decorated with the organisation's important symbols, such as eagles and swastikas frequently seen in neo-Nazi groups. Another example denotes the hanging of portraits of important figures such as Adolf Hitler and Osama Bin Laden. Furthermore, military and combat uniforms worn by important figures within the organisation as well as weapons used by them could be displayed with replicas of them available to be worn by the avatars of the current members. Finally, old and hard to find book artifacts, such as past versions of the Quaran or the Holy Bible could be offered to newly recruited members. Furthermore, digital twins along with VR/AR could assist in individuals interacting with places, buildings and geographical locations that are important to the organisation (e.g. dedicated mosque, Führer headquarters). In that way, newly recruited individuals could actively take part in present or past actions and events (e.g. praying in the mosque with members of the Taliban, ISIS or AlQueda or attend a speech by Hitler in Führer headquarters) and therefore, already feel part of the organisation. Additional examples of virtual geographical locations and buildings include concentration camps (neo-Nazi extremist organisations) or military camps of Taliban, ISIS and Al Queda. Additional examples of actions and events include the witnessing the assassination of innocent civilians and neutral military personnel, torturing captured people, participating in religious ceremonies or attending rallies and speeches of important figures within the organisation.

B. Coordination of Attacks in Physical and Cyber Space

Beyond the recruitment and radicalisation of new members and the spread of propaganda, extremists and terrorists also focus on the identification of new targets and the coordination of attacks against them. In the past, the members of the extremist/terrorist organisation needed to physically gather and decide on the targets and how the attack should be conducted. Proceeding, they would need to organise any necessary training on the members volunteering to execute the attack. With the help of VR and all the necessary information gathered, extremists and terrorists could create a highly accurate virtual representation of the environment they want to attack [27], [28]. Hence, they can train the attack team members efficiently so they succeed in the operation. Also, they can create different attack scenarios and alternative attack approaches for the members to learn in case things do not go according to plan. Hence, the attack members can gain proper training which would otherwise be impossible in the physical world. In addition, old members of the extremist/terrorist organisation can train newly recruited members to effectively interrogate, torture and execute the avatars of captured victims. In the virtual world, these tasks can easily be repeatedly reconstructed until the members in training reach an acceptable level of successfully completing such tasks. As a result, the newly recruited members can become lethal and accurate in their actions on a much faster basis and with no physical resources required. Furthermore, during the conduction of the attack in the physical world, the usage of AR could allow the attack members to quickly find their way around (e.g. virtual arrows towards the correct pathways and alternative entrance/exit points) and assist them towards their goal (e.g. identification of key figures for the operation) [27], [28].

Another aspect that is worth of consideration is how new targets become easily reachable by extremists and terrorists in the metaverse. In the metaverse, the parallel existence of whole virtual cities and their citizens has become a reality. Therefore, just as places and people can be harmed in the physical world, the same concern applies to places and people in the virtual reality of the metaverse. Extremists and terrorists can vandalise and cause damage to buildings and places that they feel goes against their ideology such as swastikas on synagogues or Jewish schools or the statues of people of colour being vandalised by white supremacists [27], [28]. Examples of buildings and places include governmental buildings (e.g. the United States Capitol, the White House, House of Parliament), places of worship (e.g. temples, churches, mosques, and synagogues), and liberal places where free speech, thinking and self-expression is accepted and encouraged (e.g. theatres, sports stadiums, cinemas, music festivals).

Similarly, various public cultural events and festivals that promote and encourage self-acceptance, self-expression, unity and respect towards others regardless of their skin colour, ethnic race, religion, sexual orientation, gender identification and financial status can be conducted in the metaverse, just as in the physical world. Similar to the previous case described, extremists and terrorists can conduct acts of hate and terrorism towards the attendees. Such unfortunate and unacceptable acts have already happened in the physical world so it is more than likely that the same acts will be conducted in the metaverse. Moreover, metaverse private ceremonies could be violently disrupted by extremists and terrorists upon their disapproval of the ceremony and the people present, such as a same-sex wedding or a wedding between two individuals with different religions or ethnic race [27], [28].

IV. Future Work and Concluding Remarks

In this study, we discussed how the metaverse could be exploited by extremists/terrorists to assist them in successfully conducting their operations. Such acts will certainly bring catastrophic consequences to individuals and communities worldwide. Although Internet 3.0, and subsequently the metaverse, will not replace Internet 2.0 overnight, protective measures should already start being developed [30]. New regulations should be introduced on what is considered appropriate, ethical and lawful behaviour without compromising the freedom of speech and self-expression [31]. In addition,legislation and policies should be constructed based on the metaverse's needs. Appropriate focus should be be given on the safety and protection of individuals from extremist/terrorist behaviour,

similarly to previous acts [32]. Moreover, with the usage of cryptocurrencies in the metaverse, extremists and terrorists can exploit the cryptocurrencies' anonymity to substantially fund themselves and avoid any financial blackslists which are inapplicable to the metaverse [33]. We should highlight that the content moderation of the metaverse will have no substantial similarities to social media and Internet 2.0 in general and the quantity of information received will be immense and difficult to manage [34]. This is ideal for extremists and terrorists as they will be free to create their own content, spread propaganda and recruit new members upon continuous radicalisation. Therefore, appropriate content moderation mechanisms should be carefully implemented [35].

Furthermore, as stated in Section II, the definitions of extremism and terrorism and their related concepts are not clear and distinct enough in different parts of the world due to geographical location, political aspects, culture, ethical standards, life views and customs [28]. In the future, universal definitions should be constructed that are fully explainable, correctly interpretable and inclusive. Finally, similarly to youngsters educated on the physical world and its threats, the same logic should be applied for the metaverse though proper education and awareness. It is vital for individuals to learn to recognise potential dangers in the metaverse, protect themselves and their peers and report to relevant authorities for any unacceptable behaviour observed.

REFERENCES

[1] J. Joshua, "Information bodies: Computational anxiety in Neal Stephenson's Snow Crash," Interdiscip. Lit. Stud., vol. 19, no. 1, pp. 17–47, 2017.

[2] R. Di Pietro and S. Cresci, "Metaverse: Security and Privacy Issues," arXiv [cs.CR], 2022.

[3] Y. K. Dwivedi et al., "Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," Int. J. Inf. Manage., vol. 66, no. 102542, p. 102542, 2022.

[4] J. Maganis, "Top companies building in the metaverse," Crowdcreate, 27-Apr-2022. .

[5] E. Dincelli and A. Yayla, "Immersive virtual reality in the age of the Metaverse: A hybrid-narrative review based on the technology affordance perspective," J. Strat. Inf. Syst., vol. 31, no. 2, p. 101717, 2022.

[6] B. Shen, W. Tan, J. Guo, L. Zhao, and P. Qin, "How to promote user purchase in metaverse? A systematic literature review on consumer behavior research and virtual commerce application design," Appl. Sci. (Basel), vol. 11, no. 23, p. 11087, 2021.

[7] J. Zhong and Y. Zheng, "Empowering Future Education: Learning in the Edu-Metaverse," 2022 International Symposium on Educational Technology (ISET), 2022, pp. 292-295, doi: 10.1109/ISET55194.2022.00068.

[8] R. Brown Sr, S. I. Shin, and J. (Joo Baek) Kim, "Will nfts be the best digital asset for the Metaverse?," 2022.

[9] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq and M. K. Khan, "Comprehensive Review of Cybercrime Detection Techniques," in IEEE Access, vol. 8, pp. 137293-137311, 2020, doi: 10.1109/ACCESS.2020.3011259.

[10] S. A. Castaño-Pulgarín, N. Suárez-Betancur, L. M. T. Vega, and H. M. H. López, "Internet, social media and online hate speech. Systematic review," Aggress. Violent Behav., vol. 58, no. 101608, p. 101608, 2021.

[11] M. Almoqbel and S. Xu, "Computational mining of social media to curb terrorism," ACM Comput. Surv., vol. 52, no. 5, pp. 1–25, 2019.

[12] S. Aldera, A. Emam, M. Al-Qurishi, M. Alrubaian, and A. Alothaim, "Online extremism detection in textual content: A systematic literature review," IEEE Access, vol. 9, pp. 42384–42396, 2021.

[13] A.-L. Watkin and M. Conway, "Building social capital to counter polarization and extremism? A comparative analysis of tech platforms' official blog posts," First Monday, 2022.

[14] M. Speicher, B. D. Hall, and M. Nebeling, "What is mixed reality?," in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19, 2019.

[15] L.-H. Lee et al., "All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda," arXiv [cs.CY], 2021.

[16] D. Schmalstieg and T. Hollerer, "Augmented reality: Principles and practice," in 2017 IEEE Virtual Reality (VR), 2017.

[17] R. Minerva, G. M. Lee and N. Crespi, "Digital Twin in the IoT Context: A Survey on Technical Features, Scenarios, and Architectural Models," in Proceedings of the IEEE, vol. 108, no. 10, pp. 1785-1824, Oct. 2020, doi: 10.1109/JPROC.2020.2998530.

[18] C. Lacey and C. Caudwell, "Cuteness as a 'Dark Pattern' in Home Robots," 2019 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI), 2019, pp. 374-381, doi: 10.1109/HRI.2019.8673274.

[19] A. Davis et al., "Avatars, people, and virtual worlds: Foundations for research in metaverses," J. Assoc. Inf. Syst., vol. 10, no. 2, pp. 90–117, 2009.

[20] Merriam-Webster. Ideology. Accessed: Oct. 10, 2020. [Online]. Available: https://www.merriam-webster.com/dictionary/ideology

[21] S. Aldera, A. Emam, M. Al-Qurishi, M. Alrubaian and A. Alothaim, "Online Extremism Detection in Textual Content: A Systematic Literature Review," in IEEE Access, vol. 9, pp. 42384-42396, 2021, doi: 10.1109/ACCESS.2021.3064178.

[22] J. J. Wisnewski, Torture, terrorism, and the use of violence (also available as review journal of political philosophy volume 6, issue number 1). Cambridge Scholars, 2008.

[23] BL Smith. (1999). Propoganda Encyclopedia Britannica. [Online]. Available: https://www.britannica.com/topic/propaganda

[24] C. McCauley and S. Moskalenko, "Mechanisms of political radicalization: Pathways toward terrorism," Terrorism Political Violence, vol. 20, no. 3, pp. 415–433, Jul. 2008, doi: 10.1080/09546550802073367.

[25] M. S. Kimmel, "Globalization and its Mal(e)Contents," Int. Sociol., vol. 18, no. 3, pp. 603–620, Sep. 2003, doi: 10.1177/02685809030183008.

[26] I. Muhammad, "Metaverse facing 'tool for terrorism' warning," BeyondGames.biz, 07-Jun-2022. [Online]. Available: https://www.beyondgames.biz/23114/metaverse-facing-tool-for-terrorism-warning/. [Accessed: 14-Sep-2022].

[27] A. C. Doctor, J. S. Elson, and S. Hunter, "The metaverse offers a future full of potential – for terrorists and extremists, too," The Conversation, 07-Jan-2022.

[28] E. d'Argenlieu, "Terrorist use of the Metaverse: new opportunities and new challenges — The Security Distillery," The Security Distillery, 12-Apr-2022. [Online]. Available: https://thesecuritydistillery.org/all-articles/terrorism-and-the-metaverse-new-opportunities-and-new-challenges. [Accessed: 14-Sep-2022].

[29] "Metaverse: Opportunities, risks and policy implications," Europa.eu. [Online]. Available: https://www.europarl.europa.eu/thinktank. [Accessed: 14-Sep-2022].

[30] A. Bosworth, F. R. Labs, N. Clegg, and Global Affairs, "Building the metaverse responsibly," Meta, 27-Sep-2021. [Online]. Available: https://about.fb.com/news/2021/09/building-the-metaverse-responsibly/. [Accessed: 14-Sep-2022].

[31] L. B. Rosenberg, "The growing need for metaverse regulation," in Lecture Notes in Networks and Systems, Cham: Springer International Publishing, 2023, pp. 540–547.

[32] D. Broeders, F. Cristiano, and D. Weggemans, "Too close for comfort: Cyber terrorism and information security across national policies and international diplomacy," Stud. Conflict Terrorism, pp. 1–28, 2021.

[33] L. Almaqableh, K. Reddy, V. Pereira, V. Ramiah, D. Wallace, and J. Francisco Veron, "An investigative study of links between terrorist attacks and cryptocurrency markets," J. Bus. Res., vol. 147, pp. 177–188, 2022.

[34] M. Wille, "No, the metaverse won't be a radical new breeding ground for extremism," Input, 13-Jan-2022. [Online]. Available: https://www.inputmag.com/tech/no-the-metaverse-wont-be-a-radical-new-breeding-ground-for-extremism. [Accessed: 14-Sep-2022].

[35] C. B. Fernandez and P. Hui, "Life, the metaverse and everything: An overview of privacy, ethics, and governance in metaverse," arXiv [cs.CY], 2022.