Human Interaction and Emerging Technologies (IHIET 2022), Vol. 68, 2022, 291–299
https://doi.org/10.54941/ahfe1002745

Addressing New Cyber Risks in Immersive Reality

Luisa Franchina, Alessandro Calabrese, Tommaso Maria Ruocco, and Giulia Inzerilli

Hermes Bay Srl, Rome 00143, Italy

ABSTRACT

The purpose of this paper is to assess the cyber risks associated with the development of Augmented Reality (AR) and Virtual Reality (VR) technologies in relation to their use in the metaverse, in the military sector and in the health sector. AR and VR represent one of the most recent and relevant technological advances that have been able to take advantage of the social changes brought about by the coronavirus pandemic and its unintended function to expedite the ongoing digital transformation across industries. This new digital reality will prospect new cybersecurity challenges and will enhance already existing digital concerns, such as security and privacy risks. As the opportunities are all encompassing, so are the cyber risks and vulnerabilities, such as identity theft, spying and social engineering. Unfortunately, new technologies are often developed and brought to market long before cybersecurity issues are addressed. Not studying the cyber paradigms in advance, not introducing minimum ethical constraints, means exposing oneself to social pathologies, which could be much more insidious than those we have experienced so far in the age of the web.

Keywords: Augmented reality (AR), Virtual reality (VR), Extended reality (XR), Metaverse, Critical infrastructure, National Security

INTRODUCTION

According to the 2021 UNCTAD Division on Technology and Logistics Report, recent developments in frontier technologies, including artificial intelligence, robotics and biotechnology, have shown tremendous potential for development in all fields of human interest (UNCTAD, 2021). Most notably, extended reality (XR) experiences that blend in-person and digital elements have seen adoption surge amid the coronavirus pandemic. Extended reality (XR) is an umbrella term for all immersive technologies including augmented reality (AR), virtual reality (VR) and mixed reality (MR). As these technologies become more exploited, we are inching closer to the era of Edge Computing, which will require tremendous processing power at the edge of the network, requiring the elaboration and the storage of huge quantities of data. One of the most significant changes in the future will regard mobility systems, which will enable people and goods to move differently, and a new class of activities characterized by the exploitation of virtual and augmented reality-based technologies that will make the physical movement of people and goods increasingly unnecessary (UNCTAD, 2021). Thanks to these technologies, it is possible to interact with a vast amount of information, with incredible effects on our personal and working lives. The prediction of all major analysis institutes is that both augmented reality and virtual reality will expand rapidly in the near future, reaching a development rate of 54% per year between 2020 and 2024 (Mozumder et al., 2022). The outlook looks very promising, not least because many global companies are well prepared to implement such solutions in-house. Globally, 82% of companies currently exploiting the benefits of augmented and virtual reality say they are satisfied with the benefits obtained (Mozumder et al., 2022). Nonetheless, the legal system, both at Italian and European level, is still in its embryonic phase, while the potential cyber risks are innumerable and already raise traditional privacy and data governance concerns such as questions of surveillance, social engineering and freedom of expression. This scenario raises two important considerations. Firstly, XR browsers facilitate the enhancement of the immersion experience, but content is created and distributed by third-party providers and applications. This raises issues of unreliability as XR is a relatively new field and the mechanisms for generating and transmitting authenticated content are still evolving. Secondly, one of the greatest perceived dangers of XR technologies concern the user's privacy as such technologies fully interact with the user. XR tools collect a lot of information about the user's identity and what they are doing, to a much greater extent than, for example, social networks or other forms of technology.

The Metaverse, an Evolving Paradigm

The metaverse is an immersive virtual world in which visual instruments and XR technologies are used to enter a space that connects all sorts of digital environments: a super virtual-reality ecosystem based on the Internet, which is composed of inter-disciplinary technologies. The term "metaverse" was coined in the mid-1990s by science fiction author Neal Stephenson (Mozumder et al., 2022). However, the word metaverse received its current popular definition from Facebook.

The speed with which technology evolves is not always matched by the normo-legal adaptation it requires. The current regulatory base at the European level, such as GDPR, NIS and NIS 2, do not provide specific references to the metaverse, and to all the implications that it will have and is having in its present applications. Nonetheless, the European Commission is supporting research and innovation into a European XR ecosystem, ensuring that our European values are upheld, as the EU is programming the applications of such technologies in the "Essential Services" sectors as highlighted in the NIS directive (UE 2016/1148). Unfortunately, this normative does not provide a reliable ground for each actor to work internally to ensure the security and resilience of its own infrastructure, especially when such activities are totally or partially diverted to virtual realities such as the metaverse. System resilience does not derive (only) from the adoption of common-sense rules on the internal perimeter but from the design characteristics of the system (Falchuk, 2018). Both when essential services use the metaverse and when they may suffer collateral damage, the attack surface, especially in times of international tension like these, increases dramatically.

The immersion of the real world in the virtual world creates nodes in which the concentration of risk is too high (single point of failure). Security risks in the metaverse take the form of new types of cyber-attacks, targeting both end-users and device endpoints, as well as operators or key service providers. In the case of attacks on system operation, this reverberates on the integrity of the system, and since the virtual universe permanently stores information online, the overall cost of the damage suffered would be greater than the current digital ecosystem (Robinson, 2022). The removal of "avatar" assets and user information in synthetic worlds would also completely negate the value of the user. The meta-universe will also generate new critical infrastructures, where damage to information storage systems would severely diminish the overall value of the virtual environment and cause huge economic losses (Garon, 2022). Therefore, the second point of reflection concerns the blockchain. There is no m etaverse without the Blockchain, because the latter acts on the decentralisation of data which is perceived to be fundamental for the metaverse to run (Grider and Maximo, 2021). Before the use of blockchain, NFTs and cryptocurrencies, everything was stored in a single database, with obvious limitations. Today, the aim is to create interoperable, secure, fast and decentralised metaverse. The blockchain is now the most suitable technology, but also an additional means of exposure to cyber threats such as identity theft and social engineering, as this technology allows, for example, to store, on a decentralized registry, the characteristics of our avatar and our digital assets (cars, clothes, real estate, digital works of art), using them in any metaverse we decide to frequent, drastically expanding our surface of digital vulnerability (Yang, 2022).

The third point of analysis concerns the protection of privacy, as the metaverse will collect more user data than ever before, drastically increasing the risk of ubiquitous monitoring and compromise of data security. In Europe, the previously announced European Data Strategy, the proposed Artificial Intelligence Regulation together with the Digital Services Act and Digital Market Act, the Data Governance Act and the recent platform-to-business Regulation, seem to be able to constitute the embryonic regulatory substrate that can be implanted in the virtual meta universe (Di Pietro and Cresci, 2021). However, even this perspective is already partial and limited, since it excludes from the regulatory framework the impact of secondary data, inferred data and non-personal data, which are fundamental for the definition of the perimeter of responsibility and governance of the metaverse. Nonetheless, there are few exceptions related to the proposed Data Governance Act, the European legal framework designed for the re-use of public sector data covered by intellectual property rights and confidential data of a personal and non-personal nature (Di Pietro and Cresci, 2021). All this has resulted in a rapid growth of criticalities, where Covid 19 has accentuated dynamics such as smart working, which, however, has been found to have both opportunities and risks: an opportunity because it has enabled a turning point in the processes of digital transformation and innovation, a risk because the digital world has become even more attractive to criminal organisations of all kinds, with objectives that belong to both the economic and geopolitical spheres (Wang, 2022). As businesses rush to plant their flag in the metaverse, not all may realize the full dangers of this new world.

The Military Paradigm, a National Defense Dilemma

Among the enabling technologies of the military industry, the family of Extended Reality (XR) technologies is becoming increasingly predominant (Stone, 2018). However, the first application of these technologies in the military field dates back to the 1930s with the first prototype of an immersive flight simulator for training aspiring pilots, called Edwin Link's Link Trainer. Since then, there have been countless applications in this field. More recently, in 2019 the US tech giant Microsoft announced its collaboration with the US Army in an agreement to prototype and test the 'IVAS' (Integrated Visual Augmentation System) system, consisting of a helmet with an augmented reality viewer, designed for both soldier training and other strategic activities. The IoT is also developing in the military sector and is increasingly referred to as the Internet of Military Things or the Internet of Battlefield Things (Göllner, 2019).

In his 2011 study "Virtual reality and its military utility", the Indian scholar Ajey Lele identified three possible applications of these technologies in the military sphere: the training paradigm, where through an immersive context, a subject can be at the helm of a fighter plane, or in a guerrilla context set in a variety of environments, learning and gaining 'hands-on' experience; in the field of medicine and surgery, where the replication of a real context can allow, for example, a military doctor to perform an operation on a wounded soldier from miles away; in the field of rehabilitation, where the simulation of a traumatic context in a controlled environment can support therapy against post-traumatic stress syndrome (PTSD) in war veterans (Livingston, 2011).

However, while there are undoubted advantages of XR technologies and IoBT/IoMT, there is a need for modern, robust and deployable defense systems that can protect the networks and the information circulating on them. This cyber dilemma has returned to the center of the public debate in connection with the Microsoft contract. While it is true that the technology could provide more and better information for the soldier to make the right decision in a real situation, the predictive system does not protect against mistakes, and it could cause very serious ones if, for example, it misidentifies a target or if the simulation is hacked and infected by activating a missile launch system, as in the case of the naval simulation. If XR technologies, as mentioned above, fundamentally represent a junction between our physical world and the virtual worlds, any cyber risks in the military realm could potentially have catastrophic consequences in the real world and compromise the national security of any state that deploys such technologies. For some Microsoft employees, there is no doubt that these technologies are 'weapons of war' in their own right, as they wrote on Twitter (Evangelho, 2019).

If one considers that the training of soldiers with augmented reality technologies is extending worldwide, one understands the need to take the ethical implications and dangers involved in the actual development of these technologies at the national level. For example, in recent years, the use of such technology by criminals and terrorist groups has become more and more pronounced and eventual hacked data of critical military infrastructures or resources could be proven to be very dangerous (Miedico, 2021). While criminals use the web for purely 'economic' and 'logistic' purposes (e.g., to launder money of illicit origin, to try to evade the classic interception systems, etc.), terrorist groups are parallelly exploiting such technological developments by recreating scenario where they can train for terrorist acts. In July 2007, a virtual headquarters of the Australian Broadcasting Corporation in the game Second Life was attacked by a terrorist group that employed spectacular urban violence, causing virtual economic damage and the virtual deaths of many civilians. Such risks are inherent to the national defense and critical infrastructures of any country who deploys such technologies (Miedico, 2021).

Furthermore, the newspaper 'The Australian' violently attacked Second Life for the presence in the game of automatic weapons and AK47s, and, among its users, of three jihadist terrorists and two elite jihadist terrorist groups capable of spreading propaganda, recruiting and instructing on how to create terrorist cells in the video game. This depiction of behavior preparatory to terrorism was underestimated by the designers, who felt that establishing direct connections between acts of 'virtual' vandalism and real terrorism was as absurd as it was unfounded. Documents made public by Edward Snowden in December 2013 showed that the US NSA (National Security Agency) and its British counterpart SIGINT (Signal Intelligence) had deeply infiltrated both Second Life and World of Warcraft for reasons of national security. These SIGINT agencies, in fact, considered these environments as potential terrorist planning and training sites, which could become even more problematic as the virtual reality becomes more efficient and accessible (Göllner, 2019).

The Medical Paradigm

The purpose of virtual medicine, or telemedicine, has initially been to minimize direct contact and impact on human body during treatment. Since then, several scientific researches have been carried out on the application of XR technologies in medicine and health care, and the interest in this field is growing due to the different medical disciplines it can involve (Mazurek, 2019). The fields of application are innumerable and include medical teaching, interactive diagnosis, preoperative planning, surgical support and assistance etc. As in the sociological and military fields, XR technologies are also used in the health sector for rehabilitation activities and psychological assessments (Caponetto and Casu, 2022).

In particular, in relation to VR technology, it represents an effective and efficient tool to plan and simulate procedures before surgery, to improve the understanding of diagnoses, to manage the relationship between doctor and patient, to visualize data and information and it also offers a revolutionary method in medical education by allowing simulation, testing and improvement of the different skills required by professionals. There are several VR system projects being implemented in this sector, the most prominent of which is Medical Reality, founded by virtual reality expert Steve Dann and

Dr Shafi Ahmend of the Royal Hospital in London. This VR system consists of a combination of 360° video and interactive 3D content that, through the use of HMDs such as Oculus and even Cardboard, allows the user to remotely witness a surgical operation through the eyes of the surgeon himself (Mazurek, 2019).

Therefore, expectations for the application of VR systems in this market are very interesting and, according to a Facts and Factors market research report in 2021, VR in healthcare will reach a value of approximately $40.98 billion USD by 2026, up from only $2.70 billion in 2020. The drastically increased demand is partially to be linked to the COVID pandemic and the strains on the health sector that followed. Further areas of application for telemedicine concern the social and economic sciences, i.e. the opportunity to use the Metaverse as an environment for observation and scientific research, and the military, as mentioned in the previous chapter (Stone, 2018).

Gartner research on a global scale shows that telemedicine is becoming a key investment driver, with 61% indicating it as their top priority, 46% assess that data management and analysis are also to be considered urgently, while IT security comes next with 42% (Clusit Report 2021). In the Italian context, it was decided to closely monitor the evolution of cybersecurity issues in the Italian healthcare market, through the "Healthcare Cybersecurity" survey carried out in our country in May 2021 to assess the status of cybersecurity efficiency in the healthcare sector. The survey reveals an overall lack of preparation in terms of both technology and professional skills. Furthermore, according to the study, 93% of healthcare companies have suffered cyber-attacks in the past, while 64% believe that a cyber-attack is likely, or highly likely, in the near future (Clusit, 2021). A healthcare facility that has not paid sufficient attention to its Cyber Security could find itself facing something worse than a simple data theft, especially when many of the activities of these facilities would be carried out in augmented reality or in virtual areas, such as the metaverse. Currently, but considering the prospect of these activities in virtual reality, a hacker could take control of an MRI machine, rendering it unusable or even dangerous for patients, increasing the intensity of the magnetic field to the point of creating burns to patients, or disabling the operating system during a remote surgery (Alder, 2020). Over the past two years, digital health has proven to be a favorite target of cybercrime with a 17 per cent increase in serious attacks worldwide between 2020 and 2021. In fact, healthcare big data is a formidable source of information that can aid treatment and prevention, but it needs to be deployed in a consistent and secure manner. Healthcare organizations collect, process and share a large amount of sensitive data and should therefore pay close attention to the security of the information they collect. In 2019, according to the results of a survey released by the HIPAA Journal, more than 38 million medical records in the US alone were exposed to a data breach (Alder, 2020). Nonetheless, data breaches do not only occur as a result of cyber-attacks. As is often the case in other contexts, they can be caused by mistakes made by internal staff, such as the use of apps not designed for telemedicine.

Within the scope of applicability of the NIS Directive (EU Directive 2016/1148), operators of essential services are called upon to contribute to the achievement of a proper security posture within the member states. As per Annexure II of Legislative Decree No. 65. of 2018, the sectors pertaining to energy, transport, health etc. are classified as operators of essential services (OSE). Nonetheless, the regulatory apparatus does not come to the rescue of individuals. Currently, at the European level, the legislation remains broad and non-exhaustive, focusing mainly on the protection of health data, through the GDPR (EU Regulation 679/2016) and the NISD (Directive 2016/1148/EU, or Network and Information Security Directive). However, security of information (data) does not equate to security of ICT systems. It is not enough to invest in technology such as antivirus software, firewalls or state-of-the-art servers to ensure information security when data is never static, but continuously travels through internal and external flows involving countless software, devices, archives, and different types of actors. The application of telemedicine and technologies such as XR and the artificial intelligences that support them are certainly revolutionary technologies, but they absolutely must be used bearing in mind the risks involved. These risks must be managed through appropriate auditing activities during the development cycle of algorithms and virtual realities, taking into account privacy, security and ethics.

CONCLUSION

Through the analysis conducted in this paper, it has been concluded that XR technologies offer a real opportunity to create a new working environment and new models of collaboration and co-operation within almost all sectors of human interest. The use of such technologies allows for the creation of collaborative layers that adopt structures and strategies to support integration between the sector of interest, suppliers, operators and partners of various kinds, and this phenomenon affects almost all companies from all the sectors considered. More specifically, virtual shared working environments extend the network structure, as in the case of scientific research, both in relation to internal and external resources, allowing the creation of highly specialized working groups by connecting geographically dispersed professionals. In this sense, it is widely believed that the use of interconnected virtual environments, thanks to the future applications within the metaverse, will lead to the development of virtual multi-sector conglomerates with high vertical and horizontal integration, stimulating both technological and economic innovation and development. However, the same qualities that make virtual reality a potentially revolutionary technology also make it profoundly dangerous. XR technologies exponentially increase the immersive qualities of the two-dimensional internet. But greater immersion means that all the current dangers of the internet will be amplified. As we move into the metaverse, as the sphere of interoperability between platforms and connected devices expands, the high break risks and the related attack surfaces increase: from authentication and access policy issues, to malware, from the reliability of encryption systems to DNS security, from DDoS attacks, to loss of data control, forgery, theft and large-scale losses, from disruption of the contextual integrity of data flows, to non-compliance with regulations. All these scenarios can potentially have real and significant personal effects, against which not even the feared solutions based on blockchain, local processing, edge computing technologies, edge servers and federated systems, would seem to provide, at least for now, more reassuring or reliable security alternatives.

REFERENCES

Alder, S. (2020), "2019 Healthcare Data Breach Report". HIPAA Journal, viewed 7 April 2022, < https://www.hipaajournal.com/2019-healthcare-data-breach-report/>.

Caponnetto, P. and Casu, M. (2022), "Update on Cyber Health Psychology: Virtual Reality and Mobile Health Tools in Psychotherapy, Clinical Rehabilitation, and Addiction Treatment." Int. J. Environ. Res. Public Health, 19, 3516.

Clusit (2021), "Rapporto 2021 sulla sicurezza ICT in Italia." *Security Summit*, viewed 7 April 2022, <https://www.mmn.it/wp-content/uploads/2021/05/Rapporto-Clusit_03-2021-web.pdf>

Di Pietro, R. and Cresci, S. (2021). Metaverse: Security and Privacy Issues. In: The Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications.

Evangelho, J. (2019), "Microsoft Employees Upset About HoloLens as U.S. Military Weapon". Forbes. viewed 7 April 2022, <https://www.forbes.com/sites/jasonevangelho/2019/02/23/microsoft-employees-upset-about-hololens-as-u-s-military-weapon/?sh=679d7dd54822>.

Falchuk, B., Loeb, S. and Neff, R. (2018), "The Social Metaverse: Battle for Privacy." IEEE Technology and Society Magazine, 37(2), pp. 52–61.

Göllner, J., Peer, A., Meurers, C. and Wurzer, G. (2019) "Virtual Reality CBRN Defence" in Meeting Proceedings of the Simulation and Modelling Group Symposium 171, pages 1–25. October 2019.

Garon, Jon M., (2022), "Legal Implications of a Ubiquitous Metaverse and a Web3 Future", Social Science Research Network, viewed 7 April 2022, <https://ssrn.com/abstract=4002551>

Grider, D. and Maximo, M. (2021), "The metaverse: Web3.0 virtual cloud economies." Grayscale, viewed 7 April 2022, https://grayscale.com/wp-content/uploads/2021/11/Grayscale_Metaverse_Report_Nov2021.pdf

Lella, I. (2021) "ENISA Threat Landscape 2021." European Union Agency for Cybersecurity (ENISA).

Livingston et al. (2011) "Military Applications of AR." Naval Research Laboratory, in Handbook of Augmented Reality, pp. 671–706.

Mazurek, J. et al. (2019). "Virtual reality in medicine: a brief overview and future research directions." Human Movement, 20(3), pp. 16–22.

Miedico, M. (2021). 'The Application of Augmented Reality and Virtual Reality Technologies in Countering Terrorism and Preventing Violent Extremism' Opening Remarks at United Nations Office of Counter-Terrorism, UNOCT, viewed 7 April 2022, < https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/20210708_statement_miedico_ar-vr_webinar.pdf>

Mozumder, M.A.I., Sheeraz, M.M., Athar, A., Aich, S. and Kim, H.C. (2022), "Overview: Technology Roadmap of the Future Trend of Metaverse based on IoT, Blockchain, AI Technique, and Medical Domain Metaverse Activity." 24th International Conference on Advanced Communication Technology (ICACT), pp. 256–261.

Robinson, J. (2022) “Exploring the metaverse and the digital future.” GSM Association, viewed 7 April 2022, <https://www.gsma.com/asia-pacific/wp-content/uploads/2022/02/270222-Exploring-the-metaverse-and-the-digital-future.pdf>

Stone, R.J. (2018), “Blending the Best of the Real with the Best of the Virtual: Mixed Reality Case Studies in Healthcare and Defence,” in Timothy Jung & M. Claudia tom Dieck (ed.), Augmented Reality and Virtual Reality, pages 277–293.

UNCTAD (2021), “Catching technological waves Innovation with equity”. *United Nations Conference on Trade and Development*, viewed 7 April 2022, <https://unctad.org/system/files/official-document/tir2020_en.pdf>.

Virca, I., Bârsan, G., Oancea, R. and Vesa, C. (2021). “Applications of Augmented Reality Technology in the Military Educational Field.” Land Forces Academy Review, 26(4), pp. 337–347.

Wang, Y., Su, Z., Zhang, N., Liu, D., Xing, R., Luan, T.H., and Shen, X. (2022), “A Survey on Metaverse: Fundamentals, Security, and Privacy.” arXiv:2203.02662.

Yang, Q., Zhao, Y., Huang, H. and Zheng., Z. (2022), “Fusing blockchain and AI with metaverse: A survey,” arXiv preprint arXiv:2201.03201.

Zhao, R., Zhang, Y., Zhu, Y., Lan, R., Hua, Z. (2021), “Metaverse: Security and Privacy Concerns.” Journal of Latex Class Files, 14(8), 1–7.