tise
transition, innovation and sustainability environments

Co-funded by the Erasmus+ Programme of the European Union

The Overview of Threats and Vulnerabilities in Metaverse

Master’s thesis for obtaining the academic degree

Masters of Science

in the study programme Transition, Innovation and Sustainability Environments

submitted by

Kamilya Issaliyeva

Department for Knowledge and Communication Management

at University for Continuing Education Krems

Advisor: Prof. Jorge M. Martins Rosa

Advisor: Prof. Marguerite Barry

Krems an der Donau, Jul 1, 2023

STATUTORY DECLARATION

I, Kamilya Issaliyeva, hereby declare,

1. that I have written my Master’s thesis myself, have not used other sources than the ones stated and moreover have not used any illegal tools or unfair means,

2. that I have not used my Master’s thesis or parts thereof as an exam paper in my domestic or any foreign country in any form to this date,

3. that, in case my Master’s thesis concerns my employer or any other external cooperation partner, I have fully informed them about title, form and content of the Master’s thesis and have his/her permission to include the data and information in my written work.

RESTRICTION OF ACCESS

ATTENTION:

The exclusion of utilisation of the Master’s thesis may be applied for to the Director of Studies (the officer responsible for the administration and enforcement of study law). A maximum of 5 years can be applied for, based on substantiated grounds that the student’s legal or economic interests are endangered if it would be published immediately.

The approval document of the accepted exclusion of utilization must be included in the bound and electronic versions of the final Master’s thesis instead of this page.

The application should be made with enough time to allow processing and return of the official document from the Director of Studies (minimum 2 months).

ACKNOWLEDGEMENTS

I would like to express my sincere appreciation to my advisors, Professor Jorge M. Martins Rosa and Professor Marguerite Barry, for their kind support and guidance throughout my Master's program. Their expertise and patience have played an instrumental role in the successful completion of this thesis, and I am truly grateful for their mentorship.

I am also grateful to the TISE Consortium for providing me with the opportunity to conduct my research and for the resources and support they have extended to me. I would like to offer special thanks to Dr. Lilya Satalkina and Kay Muehlmann for their valuable feedback during Master Thesis Seminars.

I would like to acknowledge and express my sincere appreciation to all my classmates at the TISE program. The camaraderie we shared has been invaluable, making this program all the more fulfilling. Together, we have supported, inspired, cheered for each other, and that I will never forget.

I dedicate this work to my younger self, who once doubted her ability to write even a single paragraph in English with confidence. I remember the hours spent poring over pages, searching for words in a worn-out dictionary, yet persevering despite the challenges. This accomplishment is a heartfelt tribute to the resilience and tenacity of that young girl who didn’t give up on her dreams.

I extend this celebration to all the young international students out there who face similar struggles, grappling with expressing themselves in a foreign language while confronting insecurities and fears day after day, page after page. I want you to know that I see you. Your journey is not easy, and the hurdles you overcome are commendable. Your unwavering commitment to pursue knowledge and contribute to our shared collective wisdom is truly inspiring. Let this dedication serve as a reminder that your work matters. Each word you write, each idea you share, carries significance. Embrace the journey of becoming, embrace the challenges, and know that no matter how imperfect the sentences may seem, your voice matters.

Abstract

This paper explores the concept of the Metaverse and its potential risks and vulnerabilities. The research aims to understand the nature of these risks, their potential impacts, as well as the ways in which different countries address them. The methodology combines a qualitative meta-synthesis review and a cross-country comparative analysis. More specifically, a range of sources is analysed, including academic articles, reports, policy statements and news sources. It also applies a values-based framework and cultural value orientations theory to examine the variations in cross-country regulation and governance approaches. Additionally, the paper also looks at the most affected user groups in the Metaverse. The study first discusses the transformative nature of the Metaverse and looks at its impact on various aspects of socio-economic development. After that, the potential risks associated with the integration of various technologies in the Metaverse are mapped, and cross-country case studies are assessed. The resulting findings indicate different regulatory approaches across countries and the role of tech giants in shaping the Metaverse. The research study also identifies the lack of attention given to security concerns in Metaverse development, especially with regards to the prevalent vulnerabilities of the shared digital environments for underaged users. The work acknowledges its limitations, such as the rapidly evolving nature of the Metaverse and the language barrier in accessing non-English sources. Ultimately, the findings indicate the need for a collaborative approach involving various stakeholders to ensure more-informed safety and privacy measures for all Metaverse users.

Keywords: Metaverse, Virtual Environments, Metaverse vulnerabilities, Metaverse threats

Table of Contents

1. Introduction

Although to date, there is no single, and universally aligned-upon definition of the Metaverse[1], Matthew Ball, the author of *The Metaverse: And How It Will Revolutionize Everything*, and one of the leading contemporary theorists of the Metaverse, describes it as a massively scaled interconnected network of real-time rendered 3D virtual worlds that will eventually become a getaway to most of our online experiences (Ball, 2022). As explored in one of his earlier essays *Framework for the Metaverse*, these virtual universes will be experienced "synchronously and persistently by an effectively unlimited number of users with an individual sense of presence, and with continuity of data, such as identity, history, entitlements, objects, communications, and payments" (Ball, 2020).

Unlike one might think, Metaverse will not replace the internet, but it most certainly will transform it. We will no longer simply access the internet. Instead, we will step inside of a 3D version of the internet that offers a wide range of embodied digital experiences from education and work to entertainment and trade. With such a grand vision, the Metaverse is bound to change many aspects of both the physical world and the very human life. However, although Metaverse received increased attention and investment from major tech firms all around the world, the broader impact of Metaverse remains relatively understudied from a security and privacy standpoint.

[1] In this paper, the terms "Metaverse" and “Meta worlds” refer solely to the overarching concept of the next form of virtual environment internet space that transcends individual platforms or companies. It does not specifically pertain to the commercial product or associated services offered by the American company Meta.

Thus, many questions about associated threats and potential vulnerability points in Metaverse worlds remain unanswered.

Problem Definition and Research Questions

With each new technological medium of accessing the web, comes a new improved way of harvesting user data. For its ultimate realisation and current development, Metaverse relies on a wide array of emerging technologies. In particular, artificial intelligence (AI), big data, interaction technology, virtual and augmented reality technologies (VR/AR), digital twins, cloud computing, the Internet of Things (IoT), blockchain, 3D modelling, and so on. Because Metaverse requires integration of this long list of the latest technologies and complex systems that are built on their basis, the intrinsic vulnerabilities and flaws of these existing technologies most likely will also be inherited by the Metaverse worlds. Moreover, interweaving different technologies in novel ways can amplify the existing threats like AI algorithmic bias, deep fakes, misinformation, catfishing, virtual harassment, and hijacking of wearable devices or one's cloud storage.

However, what is of particular interest to this research, due to its fundamental aspect of immersion and embodiment, Metaverse will present a unique set of its own unprecedented risks and vulnerabilities associated with biometric data, privacy, and security. Most importantly, the consequences of these threats will be more personal and immediate than the risks encountered when interacting with the current form of the internet. For example, virtual theft, harassment, identity theft, and fraud will be much more impactful when they occur in a virtual world where users feel fully present. The technologies employed for the Metaverse won't just track where users click, but they will also be able to access what they do, whom they interact with, how they interact with different users, what and how long they look at something, etc.

Every single gaze, movement, utterance can become traceable, informative, and thus valuable. As such, motivated to understand how to make Metaverse a safer space, this research is driven to explore main vulnerabilities and threats relevant for the emerging Metaverse worlds and those most affected by them. As such, the paper aims to build an understanding of the unique nature of risks that arise within Metaverse. The work also looks to map the potential impacts of these risks, while also gaining an understanding of how these vulnerabilities and risks are being addressed across different countries. Finally, the paper will look into social groups who are among the most vulnerable to potential risks in Metaverse immersive environments.

This work has been organised as follows: Section 2 describes the Research Questions guiding this study, as well as the research methods employed to investigate those questions. The next Section 3 is dedicated for introducing the background to the topic in which a historical brief related to the development of Metaverse, as well as the detailed outlook on the technologies behind the Meta worlds and Metaverse applications has been provided. In Section 4, findings from literature review are highlighted. More specifically, the Metaverse related Vulnerabilities and Threats are being discussed, alongside a comprehensive outlook on main challenges with relation to regulating the Metaverse. Finally, this section also introduces the case studies of Metaverse development and regulatory approaches across different countries. Section 5 is dedicated to the discussion of the cross-country analysis against the chosen framework, as well as analysis of main vulnerabilities and the vulnerability groups. Conclusion and outlook on limitations and further research directions have been drawn in Section 6. The glossary, tables and references can be found following Section 6.

2. Methods

The methodology for this Master's Thesis combines a qualitative meta-synthesis review and a cross-country comparative analysis. The meta-synthesis allows for the analysis of a broad range of sources, such as peer-reviewed academic articles, book chapters, government reports, statistical data from government and data gathering websites, and professional news sources. Meanwhile, the complementary cross-country comparative analysis is used to provide deeper insights into the development of the Metaverse across the selected countries. Namely, the countries include South Korea, China, Japan, the United States, and the European Union as a collective. A qualitative meta-synthesis review is particularly suitable for this study because it enables the comprehensive synthesis of diverse forms of evidence, enhancing the understanding of the research questions that frame this paper:

1. What are the main vulnerabilities and threats that exist in the Metaverse, and how are they different from the vulnerabilities of traditional Web 2.0 cyberspace?
2. What is the state of Metaverse development across different countries, and are these Metaverse-related vulnerabilities being equally addressed across different countries?
3. Who is among the most affected vulnerable groups in the Metaverse?

By systematically examining a wide range of literature, this method ensures a robust exploration of the subject matter, even when literature on Metaverse in some regions may be sparse. This event is why, when data is sparse, the review incorporates recent and relevant professional news sources to ensure the topicality of the analysis, given the rapid real-time development of the Metaverse. At the same time, the cross-country comparative analysis serves as a valuable tool to understand similarities and differences in Metaverse development and regulation across the selected countries.

This method was chosen to provide a detailed, context-specific understanding of the varied approaches to Metaverse regulation and governance, allowing for the identification of successful practices and potential shortcomings. The comparative analysis is then grounded in Kharlamov and Pogrebna (2019) human values-based framework for understanding cybersecurity regulation and governance, and Schwartz's (2006) cultural value orientations theory. These frameworks offer a nuanced lens through which to examine cross-country Metaverse regulation and governance. It allows for a culturally informed exploration of how different cultural and social value contexts influence the development of regulation in cyberspace. This paper makes a novel application of the new framework by analysing its relevance in the context of Metaverse regulations and cross-country analysis.

Through the combination of qualitative meta-synthesis review and cross-country comparative analysis, this study aims to provide a multifaceted exploration of the aforementioned research questions. The methods were chosen for the examination of a broad range of literature and in-depth case studies within a theoretical framework, ensuring a comprehensive, contextually relevant, and culturally sensitive analysis of the challenges and vulnerabilities presented by the Metaverse.

3. Background

3.1 The History of Metaverse

In June 1992, an American speculative fiction writer Neal Stephenson published his dystopian science fiction novel “Snow Crash” - a breakthrough cyberpunk imagination of the-futuristic technologies and IOT applications such as smartphones, digital currencies, mixed realities, and even VR headsets. The novel became among the first ones to describe a permanent all-encompassing cyber world that exists in parallel with the physical world. Stephenson envisions people spending more and more of their time in these digital spaces embodied by bespoke avatars, and proclaims this imagined world the **Metaverse**.

Eleven years later, San Francisco–based firm Linden Lab owned by an American computer scientist and entrepreneur Philip Rosedale made the internet’s first attempt at replicating the virtual world conceptualised by Stephenson. This project comes in a form of an online 3-D generated multimedia platform that allows avatar-embodied users to interact and socialise with each other and user-created content in real time, while relying on a thriving in-world economy, which provides opportunities to buy, sell, rent, and trade virtual items and even real estate properties using Linden Dollars. Rosedale’s creation bears a symbolic name “Second Life.”

Unlike any other video game of that time, the virtual world of Second Life allowed its residents to do a lot of those things that they previously could only experience in real life, such as shopping together, attending each other’s parties, watching movies and even allowing them experiences they couldn’t possibly actualise in a physical space such as directly creating the very world around them, be it natural landmarks, buildings or any other objects they could ideate.

Today, twenty years after its creation, Second life has attracted over two billion unique user creations and developed an impressive virtual world economy of $650 million USD (Linden Lab, 2022). Seventeen years after the establishment of the Second Life, two software developers Esteban Ordano and Ariel Meilich decided to bring the virtual world experience even further by launching Decentraland - the first Ethereum-based play-to-earn (P2E) blockchain-based virtual world powered by MANA cryptocurrency. Unlike Second Life, Decentraland is decentralised or owned by its residents and not by that world’s development team. Once created, all virtually-generated content is stored on decentralised servers that are owned by its users, and cannot be taken down by anyone. This high level of decentralisation is also made possible by smart contracts and by storing all platform transactions on the blockchain, which allows for verification by anyone and enables the creation of its virtual land parcels, called "Lands," as non-fungible tokens (NFTs). Both Second Life and Decentraland are two truly exemplary versions of the first attempt at building the Metaverse that Stephenson once defined. What might have appeared as a far-fetched sci-fi speculation two decades ago is now becoming much closer to the real world transformation of the internet.

The Metaverse, boasting more than 400 million monthly active users as of 2023, is on an upward trajectory. With the expectation of global investment climbing to an impressive $800 billion within the next five years, coupled with constant technological progress enhancing immersive user journeys, it's anticipated that by 2027, one in every four active users will spend at least an hour daily in the Metaverse (Ruby, 2023). So, what is *Metaverse* today? Although, there is still no single universally agreed-upon definition of it, the World Economic Forum gives Metaverse a following definition: “a future persistent and interconnected virtual environment where social and economic elements mirror reality; users can interact with it and each other simultaneously across devices and immersive technologies while engaging with digital assets and property” (The WEF, n.d.).

Although initially conceptualised as a single virtual world, Metaverse in its current form exists as a compilation of many different virtual worlds that have a potential to be interconnected through blockchain and Web 3.0. At the moment, more than 160 companies are building their versions of the Metaverse, with some of the most prominent among them being:

- **Epic Games:** Known for popular game Fortnite and its live virtual concerts.
- **Meta Platforms** (formerly Facebook): Currently developing its own Metaverse world and associated software, hardware, and virtual social platforms.
- **Niantic:** Developed the augmented reality (AR) mobile game Pokemon Go and utilises real-world locations and encourages physical exploration in gameplay.
- **Microsoft**: Recently made a significant entry into the gaming industry by acquiring Activision Blizzard for $67 billion and by expanding its presence in gaming and exploring opportunities within the Metaverse.
- **Decentraland:** Founded in 2017 and emerged as a pioneer in the virtual real estate trend, offering a decentralised virtual platform where users can create, explore, and monetize virtual spaces.
- **Animal Crossing:** Ran an election campaign in a virtual space, demonstrating the potential for virtual worlds to simulate real-world activities and events.

All of these companies are creating their own virtual platforms, environments, economies and universes that will combine with other virtual worlds and eventually merge with the real world to form a single Metaverse. In their paper "3D Virtual worlds and the metaverse: Current status and future possibilities" Dionisio et al. (2013) argue that in order for the metaverse to offer a single immersive and seamless virtual experience, it should ideally possess four key technical features.These are:

❖ "***Immersive realism***" which would allow the user to become emotionally engaged and fully invested in the activities of the virtual world by having a good resemblance of the physical space and simulating real-life situations and emotions.

- “***Ubiquity of access and identity***" which implies that the virtual spaces should be accessible through any digital device using a single virtual identity, regardless of the device's processing power or specifications.
- “***Interoperability***" which would allow for the smooth exchange of information and interaction between distinct systems or platforms, enabling seamless integration of different virtual environments.
- “***Scalability***" which is essential in delivering sufficient network architecture and processing power to accommodate a large number of users and real-time data exchange without compromising the system’s efficiency or the quality of users' experience.

These technical features are essential in creating an inclusive and interconnected metaverse that enables users to access a variety of virtual environments and interact seamlessly with each other. The realisation of the ultimate vision for Metaverse depends on the development and improvement of the necessary hardware and software.

3.2 Technologies behind Metaverse

Being one of the core elements of Metaverse, interoperability is a particularly central goal of the ultimate Metaverse realisation. Interoperability means that one or more meta worlds such as Decentraland and Second Life could easily interact and exchange data between each other, forming one continuous globally interconnected network. This would essentially allow Metaverse users to freely relocate their virtual assets from one metaverse to another, including NFTs and cryptocurrencies. To make interoperability a reality, Metaverse relies on a wide range of existing and emerging technologies. In particular, on the blockchain, 5G, artificial intelligence (AI), big data, interaction technology, VR, AR, MR (collectively referred to as XR), digital twins, cloud computing, the Internet of Things (IoT), blockchain, 3D modelling, and so on.

3.2.1 Blockchain

Although it is not yet a fundamental aspect of the Metaverse, ***blockchain*** and other Web 3.0 technologies will become one of the most essential pillars of Metaverse by allowing permissionless transactions necessary for interoperability, persistent identity, and immutability across multiple platforms. Blockchain, also frequently referred to as ***distributed ledger technology*** (or DLT), is a special type of database that is used to record transactions in a secure and transparent manner. This is made possible because blockchain data is stored in structures that are called blocks that are linked together chronologically. Each of these blocks contains a unique reference to the one that comes before it, forming a chain-like structure. That way, the most recent block in the chain can be easily verified by confirming that it comes after the previous block.

As a result, blockchain allows for secure and verifiable identification and transfer of virtual assets without the need for a centralised intermediary, such as a bank or government, because each block also contains a record of previous transactions. Most importantly, once the data is stored on blockchain, it is virtually impossible to modify or delete it. This is why blockchain technology can one day be used not just to secure and validate financial transactions, but also to authenticate and secure courtroom evidence in the criminal justice system, help create fully traceable and accountable supply chain management, and even increase transparency and confidence in voting during the election process. Needless to say, powered by blockchain, all of this also has a potential to eventually take place in Metaverse.

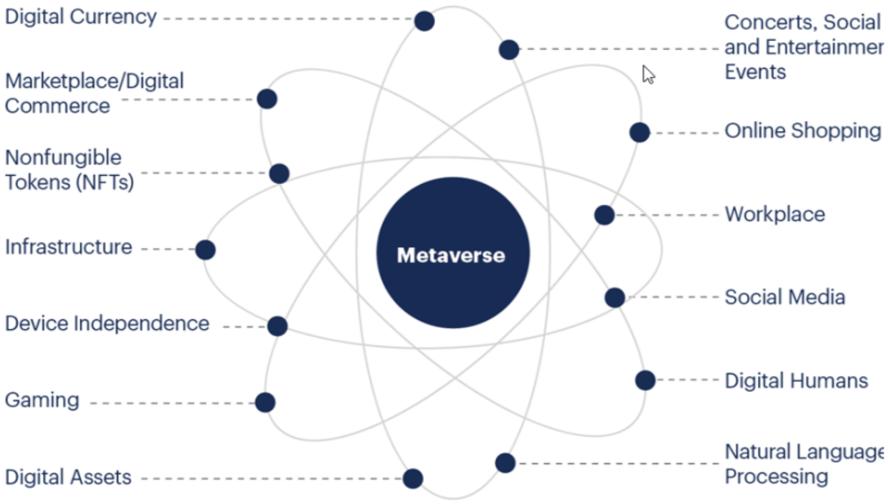
3.3 Applications of Metaverse

Although it is not yet a fundamental aspect of the Metaverse, blockchain and other Web 3.0 technologies will become one of the most essential pillars of Metaverse by allowing permissionless transactions necessary for interoperability, persistent identity, and immutability across multiple platforms. Blockchain, which is often referred to as distributed ledger technology (DLT), makes a special type of database that is used to record transactions in a manner that is more transparent and secure. This is made possible because blockchain data is stored in structures that are called blocks that are linked together chronologically. Each of these blocks contain a unique reference to the one that comes before it, forming a chain-like structure. That way, the most recent block in the chain can easily be verified by confirming that it comes after the previous block.

As a result, blockchain allows for secure and verifiable identification and transfer of virtual assets without the need for a centralised intermediary, such as a bank or government, because each block also contains a record of previous transactions. Most importantly, once the data is stored on blockchain, it is virtually impossible to either modify or delete it. This is why blockchain technology can one day be used not just to secure and validate financial transactions, but also to authenticate and secure courtroom evidence in the criminal justice system, help create fully traceable and accountable supply chain management, and even increase transparency and confidence in voting during the election process. Needless to say, powered by blockchain, all of this also has a potential to eventually take place in Metaverse.

Figure 1

Metaverse Elements



Note. From “What Is a Metaverse? And Should You Be Buying In?,” by Gartner, 2022, as cited in *Metaverse: Opportunities, risks and policy implications* | *Think Tank* | *European Parliament*. (n.d.). (https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557).

3.3.1 Healthcare

One of the industries that can be revolutionised under the influence of Metaverse is Healthcare and Medicine. Experts anticipate that as their ability to map and understand individual genetics increases, digital twinning will become possible (Sun et al., 2022). In simple terms, ***Digital Twinning (DT)*** refers to the creation of a hyper-specific and hyper-realistic virtual replica of a physical object. As the number of human genomes that are sequenced increases, it can eventually become possible for electronic health systems to house each person's digital genomic twin, which will become helpful in healthcare related decision making. With further development of the precision of this technology and by combining a variety of data sources such as medical imaging, electronic health records and genomics, Digital Twinning embedded in Metaverse can facilitate the creation of virtual personalised models of individual patients. This in turn, can result in a more precise tracking of the progression of patients' diseases and can be applied to test the efficacy of various medications and treatment options.

A recent example of DT application in healthcare was the computer simulation of patients' hearts, which was then combined with artificially intelligent algorithms to forecast the likelihood of arrhythmia (Maleckar et al. 2021). The objective of that research was to avoid performing invasive surgeries before identifying the issue and considering the alternatives. Another potential implication of DT technologies in medicine can become the discovery and precision of new drugs. Studies show that currently a significant proportion of patients, ranging from 38% to 75%, do not exhibit positive response to drug therapies for many prevalent diseases (Björnsson et al. 2020). That way, being one of the key technological elements of metaverse development, Digital Twinning can have a potential to significantly improve accuracy and precision in diagnosis, drug testing and provide personalised treatments that are tailored to each individual patient's needs.

Another technological element of Metaverse that can transform Healthcare is Blockchain. Blockchain technology can lead to decentralised management of encrypted electronic health records that can be otherwise exposed to a lot of ***data***

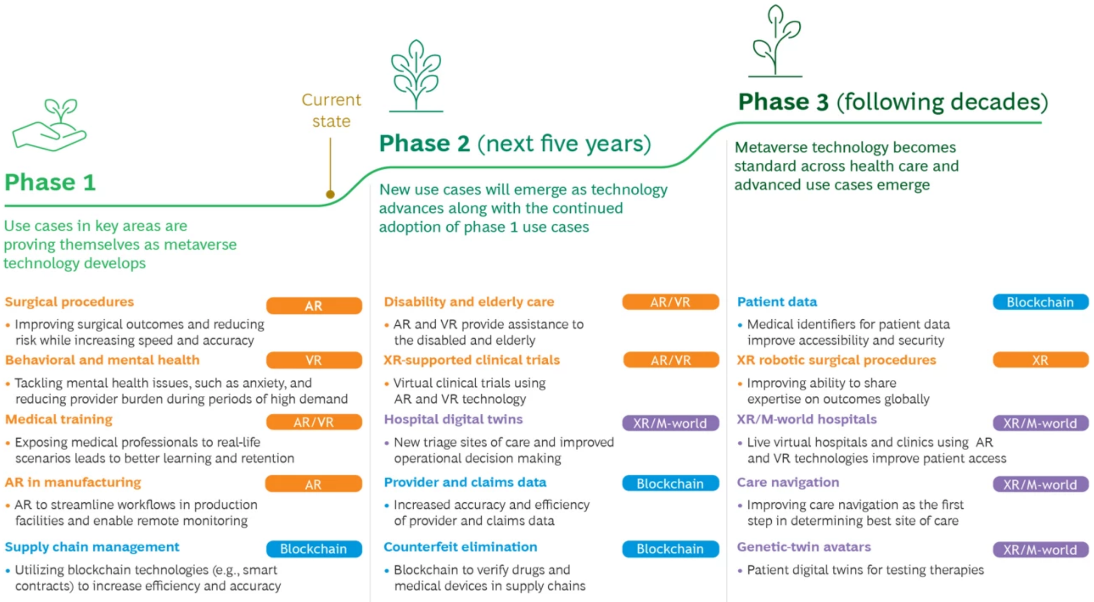
breach risks when stored on centralised servers. According to the National Institute of Health, blockchain shows promise to help electronic health records consolidate its standards, increase interoperability, and safeguard patient privacy (Shi et al., 2020). Nonetheless, some studies point out potential obstacles to implementing blockchain in healthcare. The main challenges include blockchain inefficiency created by the slow transaction processing time, which is caused by the high-complexity of computational operations, as well as the potential injustice and inequity in access and enormously high energy demands of mining (Han et al., 2022b).

Other than digital twins and blockchain, rapid improvements in VR and AR technologies offer additional opportunity for healthcare development of telemedicine consultations. The need for ***telemedicine*** became even more apparent ever since COVID-19 massively disrupted in-person patient care. According to some reports, there has been a drastic increase in global financial investments in virtual care and digital healthcare, which has triggered further innovation in the industry leading to venture capitalist digital health investments rising threefold in 2020 in comparison to 2017 (Market, 2022). At the moment, most of the existing telehealth solutions are primarily focused on psychiatry, substance use disorder, endocrinology, and rheumatology specialties (*Telehealth: A Quarter-trillion-dollar post-COVID-19 Reality?*, 2021). Nonetheless, McKinsey and BCG predict that as investments continue to rise and regulations allow for more XR technologies in hospital care, the industry will see more novel applications of telemedicine solutions (See Table 1).

For instance, future of telemedicine can look like a hybrid mode of medical procedures where surgeons are able to perform real-time operations remotely with mixed reality headsets and high-precision remote telecontrol surgical tools, real-time AI language localisation in medical operations to allow for remote cross-border international collaboration, VR supported medical trainings, blockchain-enabled standardised encrypted provider and claims data, and increased availability of teleconsultations with a wide range of healthcare professionals. In conclusion, Metaverse has the significant potential to transform the global healthcare and medicine industry with Digital Twinning, Blockchain, and VR/AR technologies being the central elements that offer opportunities for personalised treatments, improved diagnosis and disease monitoring, standardised patient data, as well as XR-enabled medical procedures and consultations (Table 1).

Table 1

New Use Cases Will Emerge As Metaverse Develops



Phase 1

Use cases in key areas are proving themselves as metaverse technology develops

Current state

Surgical procedures AR

- Improving surgical outcomes and reducing risk while increasing speed and accuracy

Behavioral and mental health VR

- Tackling mental health issues, such as anxiety, and reducing provider burden during periods of high demand

Medical training AR/VR

- Exposing medical professionals to real-life scenarios leads to better learning and retention

AR in manufacturing AR

- AR to streamline workflows in production facilities and enable remote monitoring

Supply chain management Blockchain

- Utilizing blockchain technologies (e.g., smart contracts) to increase efficiency and accuracy

Phase 2 (next five years)

New use cases will emerge as technology advances along with the continued adoption of phase 1 use cases

Disability and elderly care AR/VR

- AR and VR provide assistance to the disabled and elderly

XR-supported clinical trials AR/VR

- Virtual clinical trials using AR and VR technology

Hospital digital twins XR/M-world

- New triage sites of care and improved operational decision making

Provider and claims data Blockchain

- Increased accuracy and efficiency of provider and claims data

Counterfeit elimination Blockchain

- Blockchain to verify drugs and medical devices in supply chains

Phase 3 (following decades)

Metaverse technology becomes standard across health care and advanced use cases emerge

Patient data Blockchain

- Medical identifiers for patient data improve accessibility and security

XR robotic surgical procedures XR

- Improving ability to share expertise on outcomes globally

XR/M-world hospitals XR/M-world

- Live virtual hospitals and clinics using AR and VR technologies improve patient access

Care navigation XR/M-world

- Improving care navigation as the first step in determining best site of care

Genetic-twin avatars XR/M-world

- Patient digital twins for testing therapies

Note. From “The Expanding Health Care Metaverse,” by M., Mérey, T., Adigozel, O., & Busch, N., *BCG Analysis*, 2023 (https://www.bcg.com/publications/2023/the-expanding-reality-of-the-health-care-metaverse).

3.3.2 Education

The world of Metaverse has the potential to alter lives of not only businesses, patients and healthcare providers, but also students and children. The education sector can gain significantly from the Metaverse technologies with benefits that range from immersive learning experiences, increased learning speed, a more inclusive learning and teaching environment, and the ability to acquire highly engaging hands-on experience. There is a growing body of literature that suggests that virtual learning environments have shown to be effective in teaching young students difficult learning materials, particularly within STEM fields (Paxinou et al., 2020; Broisin et al., 2017; Kennedy-Clark, 2011; Chou et al., 2001). Some studies find that AR and VR technologies are helping students to visualise abstract concepts that would be otherwise challenging to comprehend (Sahin and Yilmaz, 2020; Hite et al., 2019).

Another study, that looked at middle- school students, found that having a whole-body, mixed reality simulation learning environments that engages the physical body in virtual space leads to increase in levels of learning and student engagement, as well as a formation of a more positive attitude towards the subject (Lindgren et al., 2016). Utilising the power of the XR technologies, Metaverse can also transform the traditional classrooms into an immersive virtual learning playground that allows for otherwise expensive experiences and experimentations. The entire science laboratories can be filled with all of the state of the art equipment that the schools wouldn’t be able to afford otherwise. This way, Metaverse learning environments can incorporate fun and engaging gamification. They also allow for material and learning techniques personalisation, as well as creating a space for a more inclusive collaborative space for students and lecturers of different abilities and backgrounds.

One of the existing Metaverse worlds that provides an opportunity for educational organisations to launch their schools and institutes in meta space is Engage. In January 2023, Engage presented the world's first fully featured film school that utilises the features of VR for teaching all stages of filmmaking from script writing to using film hardware to setting up shots. The virtual institution prioritises ensuring that all students have access to fully furnished, completely immersive virtual studios, greenrooms, and multi-camera production environments. It is marketed as a program that offers direct hands-on experience with advanced "virtualized" film-making equipment, including a motion capture stage, accessible to individuals irrespective of their geographic location (*Metaverse Company Virtual Film School - ENGAGE | the Professional Metaverse Platform*, 2023).

Another example of existing educational opportunities in virtual space is “Minecraft Education Edition”. This Minecraft platform utilises the appeal of game-based learning to enable educators globally to construct engaging lessons within a digital realm, leveraging children's enthusiasm for interactive experiences and Minecraft. Already hosting over 500 lesson plans, the platform caters to a wide array of subjects, from traditional ones like Math and Science to more contemporary topics like "Climate & Sustainability" and "Social and Emotional Learning" (*What Is Minecraft Education?*, n.d.).

When applied with precision and thoughtfulness, Metaverse has the potential to improve and revolutionise the educational experience as a whole. The whole-body mixed reality simulation environments could also promote faster, more efficient, and more engaging knowledge retention, foster an environment of inclusivity for all, and enable the acquisition of practical skills in affordable, safe, and controlled environments. Nonetheless, some challenges with the existing forms of technology and innovation remain. One of such challenges is cross-platform compatibility because as the number of Metaverse worlds grow, there would be a need to make it easier for its users to move across the platforms and collaborate with each other across different Metaverse environments.

Another opportunity and challenge is inclusivity. While Metaverse can promise more inclusivity for students who wouldn't otherwise be able to travel and learn from renowned lecturers from across the world, the initial access to the technology itself remains to be an obstacle for many people with limited access to the internet, electricity, tech or digital literacy. As some students would be able to attend the new form of virtual and immersive classrooms, there still would be many of those who wouldn't be able to afford entering the Meta space. This new form of virtual learning divide needs to be addressed further in the discussion on Metaverse.

3.4 Metaverse as a Disruptor

Unlike one might think, Metaverse will not replace the internet, but it most certainly will transform it. We will no longer simply access the internet. Instead, we will step inside of a 3D version of the internet that offers a wide range of embodied digital experiences from education and work to entertainment and trade. With such a grand vision, the Metaverse is bound to change many aspects of both the physical world and the very human life. However, although Metaverse received increased attention and investment from major tech firms all around the world, the broader impact of

Metaverse remains relatively understudied from a security and privacy standpoint. Thus, many questions about associated security and privacy risks remain unanswered.

4. Results

4.1 Literature Review

In order to address the gap in existing literature, this study looks deeper into the challenges and vulnerabilities of Metaverse as an emerging virtual cyberspace. To achieve this, a range of literature resources is utilised, including academic papers, industry reports, books, government documents and press releases, investigative journalistic pieces, expert opinions and reputable news articles (Table 2). The aim was to gather a diverse set of perspectives and evidence-based insights on the issues and vulnerabilities, as well as regulatory challenges associated with underlying technologies. As a result, this section provides a foundation for understanding the current state and potential vulnerability areas in the ecosystem of Metaverse.

Table 2

Types of Literature Resources Used in This Study

Literature	Examples
Academic papers	Pavlou (2011); Nguyen et al. (2021); Nissenbaum (2009); (Larkina, 2022)
Books	“Privacy in Context: Technology, Policy, and the Integrity of Social Life” by Helen Nissenbaum; “Without a Net: Librarians Bridging the Digital Divide” by Jessamyn West
Reports and statistics	World Economic Forum (WEF) reports
Legal documents and regulations	European General Data Protection Regulation (GDPR)
Industry insights	Epic Games; Meta Platforms; Kaspersky

Government documents and policies	South Korean government Metaverse strategy document; ethical roadmap
Press releases	South Korean Ministry of Science and ICT press releases
Online articles	CoinTelegraph; PR Newswire

Note. From “The Overview of Threats and Vulnerabilities in Metaverse” by Issaliyeva (2023).

4.1.1 Threats in metaverse

Data Privacy Risks

The amount of personal information that is being collected, shared, and monetised in the current version of Web 2.0 makes data privacy a critical issue in the context of potential user vulnerabilities in evolving cyberspace. The World Economic Forum estimates that by the year of 2025, 463 exabytes of data will be produced each day globally – that number is equivalent to 212,765,957 DVDs created per day (World Economic Forum, 2020). All of that ocean of data can be exposed to potential data privacy concerns. Although, as Pavlou (2011) points out, there is no single universally agreed-upon definition of the term and its elements, ***data privacy*** is mostly referred to the right of a citizen to have control over how their personal information is being collected, stored and used (Emotiv, 2022). Similarly, the European ***General Data Protection Regulation (GDPR)*** privacy and security law highlights the importance of protecting individuals' privacy rights and extends those rights to object the processing of data, as well as the right of accessing, correcting, and deleting any of the personal data that was already collected (GDPR, 2016, Chapter 3).

In her book *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Helen Nissenbaum argues that privacy is not only important on an individual level for protecting one’s autonomy and personal dignity, but it is also crucial for sustaining effective social institutions and maintaining trust between society and these institutions, along with fostering of shared social norms and values (Nissenbaum, 2009). As such, it is important to have a further outlook on privacy vulnerabilities in the context of evolving Metaverse and associated technologies not only for its implication on individual user rights, but also to understand how privacy threats in virtual space can have a larger spillover impact on social cohesion and institutional strength.

The World Economic Forum projects that by the end of the decade, the Metaverse will reach 700 million people worldwide (World Economic Forum, 2023). With wider adoption of meta technologies and given the highly immersive nature of the experience, the relevance of data privacy related issues in the context of virtual cyberspace will remain high. Due to its disruptive and innovative nature, Metaverse will handle an unprecedented amount of user, business, and institutional data. The new ***3D environments*** of Meta universes will create a new layer of data collection and analysis that is far more advanced than the data currently harnessed by conventional social media sites.

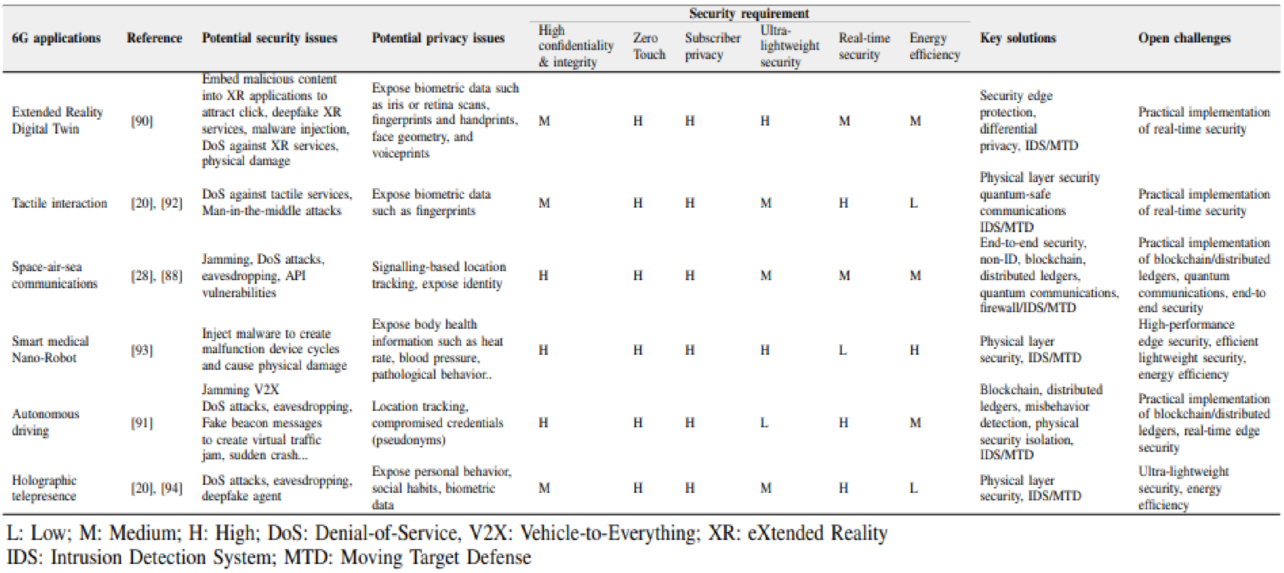
Kaspersky, a cybersecurity firm, issued a warning in their report "Consumer cyberthreats: predictions for 2023" on November 28th, indicating that the metaverse is expected to be exploited more due to the absence of necessary data protection and moderation regulations (Larkina, 2022). A significant reason why the data privacy threats will increase is due to the emerging technologies that are at the base of the Metaverse infrastructure. For example, in their paper “Security and privacy for 6g: A survey on prospective technologies and challenges,” Nguyen et al. (2021) discuss how Extended Reality (XR) and Digital Twin technologies can raise a potential privacy issues by exposing sensitive biometric data such as face, iris and retina scans, fingerprints, heart rate and unique voiceprints (Table 3).

Consequently, a user will no longer only be exposed to malicious data leaks with regards to their personal passwords, social security or credit card information, but also when it comes to a whole new layer of highly sensitive permanent biometric data that can’t be changed and is unique to every individual. This is why such data is regarded as highly sensitive ***Personally Identifiable Information (PII)***. Nguyen et al. (2021) conclude that this type of privacy vulnerabilities can lead to potential security issues such as ***malware injections***, malicious deepfake XR services, ***DoS against***

XR services, ***Man-in-the-middle attacks***, ***eavesdropping***, ***DoS attacks*** and even physical damage.

Table 3

Security and Privacy Issues of Several 6G Applications



6G applications	Reference	Potential security issues	Potential privacy issues	Security requirement						Key solutions	Open challenges
				High confidentiality & integrity	Zero Touch	Subscriber privacy	Ultra-lightweight security	Real-time security	Energy efficiency		
Extended Reality Digital Twin	[90]	Embed malicious content into XR applications to attract click, deepfake XR services, malware injection, DoS against XR services, physical damage	Expose biometric data such as iris or retina scans, fingerprints and handprints, face geometry, and voiceprints	M	H	H	H	M	M	Security edge protection, differential privacy, IDS/MTD	Practical implementation of real-time security
Tactile interaction	[20], [92]	DoS against tactile services, Man-in-the-middle attacks	Expose biometric data such as fingerprints	M	H	H	M	H	L	Physical layer security quantum-safe communications IDS/MTD	Practical implementation of real-time security
Space-air-sea communications	[28], [88]	Jamming, DoS attacks, eavesdropping, API vulnerabilities	Signalling-based location tracking, expose identity	H	H	H	M	M	M	End-to-end security, non-ID, blockchain, distributed ledgers, quantum communications, firewall/IDS/MTD	Practical implementation of blockchain/distributed ledgers, quantum communications, end-to end security
Smart medical Nano-Robot	[93]	Inject malware to create malfunction device cycles and cause physical damage	Expose body health information such as heat rate, blood pressure, pathological behavior..	H	H	H	H	L	H	Physical layer security, IDS/MTD	High-performance edge security, efficient lightweight security, energy efficiency
Autonomous driving	[91]	Jamming V2X DoS attacks, eavesdropping, Fake beacon messages to create virtual traffic jam, sudden crash...	Location tracking, compromised credentials (pseudonyms)	H	H	H	L	H	M	Blockchain, distributed ledgers, misbehavior detection, physical security isolation, IDS/MTD	Practical implementation of blockchain/distributed ledgers, real-time edge security
Holographic telepresence	[20], [94]	DoS attacks, eavesdropping, deepfake agent	Expose personal behavior, social habits, biometric data	M	H	H	M	H	L	Physical layer security, IDS/MTD	Ultra-lightweight security, energy efficiency

L: Low; M: Medium; H: High; DoS: Denial-of-Service, V2X: Vehicle-to-Everything; XR: eXtended Reality
IDS: Intrusion Detection System; MTD: Moving Target Defense

Note. From "Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges," by Nguyen, V., Lin, P., Cheng, B., Hwang, R., & Lin, Y. , 2021, *IEEE Communications Surveys and Tutorials*, 23(4), 2384–2428, p.10. (https://doi.org/10.1109/comst.2021.3108618).

Identity Theft and Impersonation

One of the ways in which the personal and biometric data vulnerabilities of Metaverse can be exploited is through identity theft and virtual impersonation. ***Identity theft*** can be defined as the intentional and unauthorised use of someone's personal identifying information for one's own benefit or unlawful purposes (Federal Trade Commission, 1998, Koops and Leenes, 2006). Irshad and Soomro (2018) identify several types of low technology and traditional identity theft that includes medical, tax, financial, synthetic, driver's licence and even child identity theft, which targets stealing minors' personal data. Meanwhile, ***digital impersonation*** is a more recent phenomenon that became common with the introduction of cyberspace and social media. It is an act of deceiving to be someone else by assuming the real identity of another person, either by hacking that user’s account or by creating a new user profile that posts new content and replicates the original identity by copying their visuals, language, and behaviour for malicious purposes (Zarei et al., 2020).

Even in today's era of Web 2.0, one’s online identity remains a major vulnerability point to cybercrime. This threat, however, is not limited to individuals but also extends to businesses. According to a study conducted by the Identity Defined Security Alliance (IDSA) in 2020, 79% of the organisations surveyed had suffered from a data breach related to identity theft within the past two years. The situation appears to have deteriorated further as a follow-up survey in 2022 revealed that the number had risen to 84% of respondents companies experiencing an identity-related data breach within the previous year (MIT Technology Review, 2022). This alarming trend can be mirrored and possibly aggravated in the virtual worlds of metaverse. In years to come, the immersive and all-encompassing virtual nature of the metaverse may pave the way for a new, more intricate and sophisticated type of identity theft or impersonation.

In his interview to Cointelegraph, Andrew Newman, an CTO and co-founder of cybersecurity firm ReasonLabs and former architect of Microsoft’s Windows Defender anti-malware software, confirmed this projection. Newman warned: “As our real-life and online identities continue to merge, the stakes for identity theft on the Metaverse will increase” (Young, 2022c). He also shared that there already were reported cases of impersonation related avatar scams on big metaworlds such as Roblox. Hackers can manipulate users into getting access to their virtual avatars in order to receive an access to their actual personal identity information or to obtain an access to their valuable virtual crypto assets.

Attackers can also implant features to deceive the users into sharing their personal information unknowingly. In a world where anyone can be embodied through a virtual avatar that can take any shape or form, how do you know who or what is behind the objects in your virtual environment? A hacker can create a spying bot that would look just like an ordinary lamp or a chair in the virtual conference room of your next business meeting. The power of Metaverse is that anyone can become anything.

This presents another ***metacrime*** opportunity for ***ransomware attacks***, where the hackers can threaten the user, business or the platforms to disclose their personal information until they are paid off.

In his article “Digital doppelgängers and evil twins: How brands can guard against identity theft and fraud in the metaverse”, Michael Ringman proposes 3 groups to distinguish different Metaverse cybercriminals who use impersonation and identity theft techniques for fraudulent activities. He names them evil twins, digital doppelgängers, and virtual phishing scammers (Ringma, 2023). While evil twins deceive users into thinking that they interact with another person or a brand that is already trusted by that user, digital doppelgängers are fraudulent virtual avatars that appear to be the user. Meanwhile, virtual phishing scammers trick users into entering a metaverse that seems to be real but is actually a fake virtual world where their victims would unknowingly share their sensitive information.

Additionally, the growing use of machine learning technologies paired up by the availability of unique biometric data stored by the IOT devices that support Metaverse allows for the alteration of one’s voice, speech patterns, movements, looks, behaviour and even emotional fluctuations while retaining its authenticity. So if a hacker was to obtain the sensitive biometric user data from a VR headset or other wearables and IOT devices, they could potentially use it to construct a digitally manipulated synthetic media duplicate, commonly referred to as a ***deepfake***, thereby undermining the validity of digital identity verification in Metaverse. This makes it easier to then impersonate someone in order to conduct malicious, unlawful and fraudulent cybercrime with serious real-world repercussions.

Deepfakes can cause significant damage beyond the scope of an individual user. One example of the scope of corporate damage that deepfakes can inflict is the 2020 case of the $35 Million bank heist that became possible when cybercriminals convinced a bank manager in Hong Kong to authorise the transfer of money because he received the instructions directly from the director of the company (Brewster, 2021). The manager had no reason to doubt his director because it was exactly his voice over the call, only that the voice he heard was a form of a perfect identical synthetic replica of the original voice that became possible through the autoencoder neural network behind the deepfake technology. Research has also looked at how cybercriminals can also apply deepfakes to impersonate celebrities, social influencers, and even politicians to manipulate public perceptions and opinions (Fallis, 2020; Vaccari & Chadwick, 2020; Westerlund, 2019). As more businesses, hospitals, law firms, education centres and political institutions will relocate into Metaverse, malicious deepfakes in Web 3.0 can also translate into mass public disinformation.

Disinformation and Public Deception

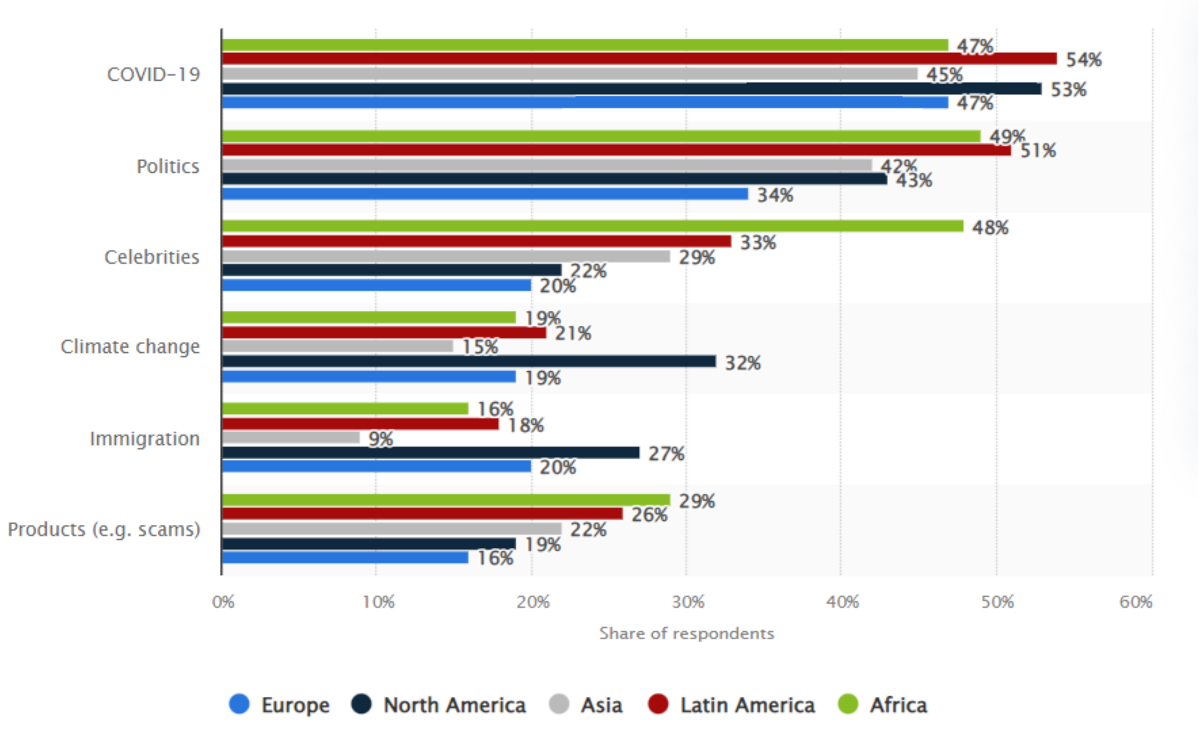
Misinformation is defined as a form of false, inaccurate or misleading information that was created with deliberate intentions, however, can be spread either intentionally or unintentionally (Wu et al., 2019b). A related term that is often used in the context of misinformation is ***disinformation***. Similarly, it refers to the persistent misleading or falsified information with the only difference in the malicious intention behind its dissemination. Nonetheless, accurate and factual information can also be manipulated by being intentionally applied in different contexts to mislead or inflict harm upon a person or a group of people, which is referred to ***malinformation***. The discourse on misinformation and disinformation became dominant in academic research and the public arena with the rise of social media. It is especially given particular attention in the context of political campaigns, elections and COVID-19 matters. For example, Wasike (2022) and Helmus et al. (2020) examined the persuasiveness of memes that were used to shape public perception towards masks and vaccines during the pandemic, while DiResta et al. (2019) and Wong, Shepherd, and Liu (2019) studied how Russia and China turned to social media material as a tool to manipulate public opinion regarding elections, political campaigns and protests.

Consistently, a worldwide study conducted by Statista in early 2022 found that between 45 and 54 percent of respondents had encountered either fake or misleading news related to COVID-19 pandemic in the week running to the survey, with the second most prominent source of misinformation and disinformation being political news (Graph 1). The regions most exposed to the falsified information were

Latin America, Africa and North America (Statista, 2022). Even with more AI content moderation efforts put in place by platforms such as Instagram, Facebook and Twitter, the spread of false information remains on the rise. In their 18th edition of Global Risks Report, the World Economic Forum warned that as cybersecurity will remain to be a pressing issue among all of the countries, the widespread implementation of new technologies have a potential to exacerbate the existing inequalities and deepen the level of misinformation and disinformation found on the internet (World Economic Forum, 2023). As a long-term global risk, the same report gives misinformation the ranking of 11 by the level of intensity of its anticipated severity, coming right after the risks of Large-scale environmental damage incidents and Geoeconomic confrontation.

Graph 1

News consumers who saw false or misleading information about selected topics in the previous week worldwide as of February 2022, by region



Note. From “Consumers witnessing false information on certain topics worldwide 2022, by regions,” by Statista, 2022b, June 28 (https://www.statista.com/statistics/1317019/false-information-topics-worldwide/).

The scale and impact of disinformation is expected to grow with the expansion of automation and machine-learning applications, from the deepfakes discussed in the previous chapter to the advanced natural language processing bots that imitate human-written text, similar to the GPT-4 foundational large language models (LLMs) used at Open AI. Left unaddressed, the issue of disinformation will be aggravated once moved to the realm of virtual reality in Metaverse. Social media is already allowing for our personal data to be used by data brokers and third parties in order to alter our experience of the content we engage with through personalised integrated advertisement that blends into our news feeds. While one might think that they are exposed to the same information as everybody else, the algorithms that reward the clickbait behaviour push users into ideological echo chambers (Cinelli et al., 2021b).

All of this will be amplified in a virtual environment where integrated advertisement will reach a new level of power to deliver a seamless and customer-centric subliminal messaging. Instead of seeing advertisements in your feed, where one now expects to find it today, the Metaverse ads would be able to penetrate your entire virtual environment, dictating what you would see on the streets, at your office, in the privacy of your virtual home or on other avatars. In his interview to the Insider, Shawn Frayne, the Chief Executive Officer of holographic company Looking Glass Factory, shared his concern regarding this change, saying: “If you think Facebook on your phone has been bad for democracy, think about your entire field of view controlled by a company like that" (Canales, 2021).

Another insight on the topic came from Rand Waltzman, a senior information scientist at the American research institution RAND Corporation, who spent four decades working on problems of AI, deception, and disinformation. Waltzman identified that when it comes to emotional manipulation, which is often abused as a strategy in effective misinformation and disinformation cases, there are two features of the Metaverse that make it vulnerable to such threats — presence and embodiment (Waltzman, 2022). Waltzman refers to “***Presence”*** as a false perception of VR and AR users about their ability to communicate with one another directly without any form of intermediary computer interface or third party agents. Meanwhile, ***“Embodiment***” means that the same user has the feeling that their virtual avatar or virtual body is their actual body. When experienced in combination, presence and embodiment can distort one's perception of the Metaverse as a reality.

The problem with this is that such reality replicas would be highly customisable and curated for each individual's tastes. On their walk to the office, two avatars can be walking down the same Metaverse street, one can pass by a gun shop, while another by an abortion clinic. The content you will see in your augmented reality will be tailored to reinforce your personal beliefs, while giving you a false impression that your reality is still a shared reality. Having these two avatars make an informed socio-political decision that will have a direct impact on their real physical realities would become ever so difficult because the very perception of their immediate environment and the common reality in which they operate will be fundamentally different. As such, what makes it different from our current experience of Web 2.0 echo chambers is that we will no longer be exposed to different informational bubbles about the same reality, we will be living different realities. If that becomes the case, how do we build a public dialogue or achieve collective action on pressing issues that affect our common neglected physical reality if our fundamental perception of reality undergoes such significant transformation?

Economic Disparities and Virtual Exclusion

Today technology has often been hailed as an equalising force that provides access to opportunities and resources, thereby bridging socioeconomic disparities (Arsić, 2020; Spulbar et al., 2022). However, although it does in fact bring a myriad of opportunities and socio-economic progress, the chasm between the digitally privileged and the digitally underconnected remains an important problem. According to recent statistics published by Geneva Digital Watch observatory, as of 2022, approximately 66% of the global population had internet access, while the remaining 34%, which constitutes roughly 2.7 billion people, are still unconnected to the digital world (Digital Access in 2023 - DW Observatory, n.d.). This lack of access to the benefits that come from utilisation of emerging technologies including as Augmented Reality, AI and Big Data, combined with the increasing reliance on more internet of things (IOT) devices and high internet connectivity systems, exacerbates the existing divide between the haves and have-nots of the underprivileged population. This disparity in digital access is commonly referred to as the ***digital divide***.

As defined by American library technologist Jessamyn West in her book *Without a Net: Librarians Bridging the Digital Divide*, the digital divide is a simplistic term used to describe the gap between those who have easy access to technology, and those who do not (West, 2011). In her book she argues that this disparity has existed for over a decade, perpetuated by various factors such as inadequate internet access, economic disadvantages, the gap between the rural and urban infrastructure development, as well as the low level of technological literacy and proficiency among the elderly and ethnic minorities. West advocated that the historical and systematic inequalities should also be assessed to build a comprehensive understanding of the root cause of technological exclusion. Indeed, as reported by the International Telecommunication Union, while the internet penetration rate amounts to 87% in the developed nations, the number falls to 47% in developing countries and reaches only 19% in the least developed countries (International Telecommunication Union, 2022). Digital divide is an important topic for discussion in the context of emerging technologies because as more industries adapt the technology to reap the benefits of innovation, the more likely inaccessibility of it will put others at economic, social and intellectual disadvantage.

The internet connectivity and digital divide has already shown to be a significant barrier to remote work and online participation for many professionals and students who didn't have adequate access to online or physical resources and yet were forced to relocate to cyberspace over the period of COVID-19 (Eruchalu et al., 2021; Lai & Widmar, 2021; Watts, 2020). Similarly to high demands for online connectivity over the pandemic, Metaverse has a potential to become another industry disruptor by causing a significant shift in patterns of consumption, investment, education, business, and socioeconomic activities. There are several factors that can contribute to the digital divide in the Metaverse, including the internet penetration, reliable 6G infrastructure, digital literacy, and the cost of technology that would allow for easy access to virtual worlds and better user experiences. It is important to acknowledge that these issues are not new, but they still may be exacerbated in the emerging context of the Metaverse, which has the potential to become a significant force in shaping the new norms of internet and virtual interaction. As such, to ensure equitable access and participation in the Metaverse, digital divide is an important factor to include in the discussion on the potential threats and vulnerabilities in the era of Meta worlds.

In addition to other factors, the high costs of supporting technology remains a significant barrier to entry for many of those who can't afford the cost of the gear. To have a fully immersive experience, one needs to purchase the VR headset, a powerful computer or mobile device with high-performance specifications to run the necessary software and afford the bandwidth, as well as peripheral devices such as hand controllers and sensors that can help enable further seamless and precise interaction with the virtual world. The current price of the 256GB Meta Quest 2 starts from $499.99 and goes up to $1,499.99 for the higher-end Meta Quest Pro.

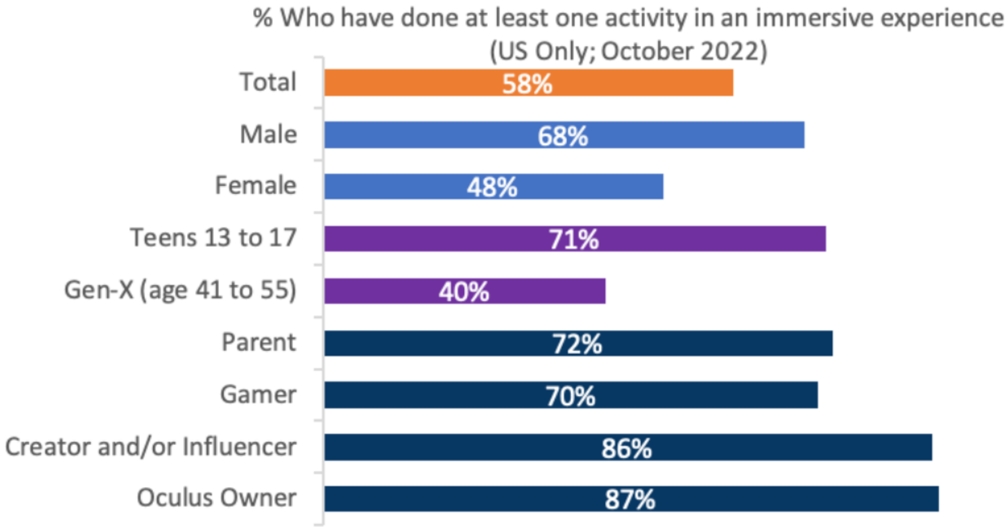
Meanwhile, those who want to have a mixed reality experience opt for Microsoft Hololens 2 which currently retails for $3,500 (*HoloLens 2—Pricing and Options | Microsoft HoloLens*, n.d.). These products are priced high enough to remain out of reach for a lot of people. In fact, according to the recent study conducted by Ipsos for the World Economic Forum, one in three (34%) of global respondents indicate that, for them, the greatest barrier to engagement with Metaverse is the cost of the technology and 20% indicate the cost of the experiences and add-ons to be a considerable financial limitation (*Are Immersive Experiences Creating a New Digital Divide?*, 2023). Aron Solomon, the Chief Legal Analyst for digital marketing agency Esquire Digital, in his interview to Lifewire, shared a similar concern, saying: “If the Metaverse is the Wild Wild West, you ideally want the best horse and saddle you can afford" (Sharma, 2022).

So who are the people most likely to be excluded from this experience? While it is hard to make high probability predictions about the future scenarios, we can observe who is currently affected by the digital divide in the metaverse. The same 2023 Ipsos study for the WEF asked respondents from China, Saudi Arabia, the UAE, UK and the US whether they think that “metaverse is for people like me”. The findings showed that 53% of Chinese agree with the statement, similarly to 52% of Emirati respondents, which goes in contrast to only 27% of the UK citizens sharing the same notion (*Are Immersive Experiences Creating a New Digital Divide?*, 2023). More interestingly, the study revealed wide and diverse differences among demographic subgroups. Mainly, differences in opinions by age, with a clear line drawn between those over 40 and those younger (Graph 2).

For example, for the US only 30% of people between the ages of 41 to 55 feel like there is a space for people like them in Metaverse, while more than half of those aged from 13 to 17 and 31 to 40 felt more comfortable to join the virtual space. A potential explanation for such drastic differences in attitudes towards Metaverse by age groups can be the level of digital literacy about the technology and its current forms of applications, which are still widely promoted in gaming and entertainment.

Graph 2

Percentages of those who have done at least one activity in Metaverse.

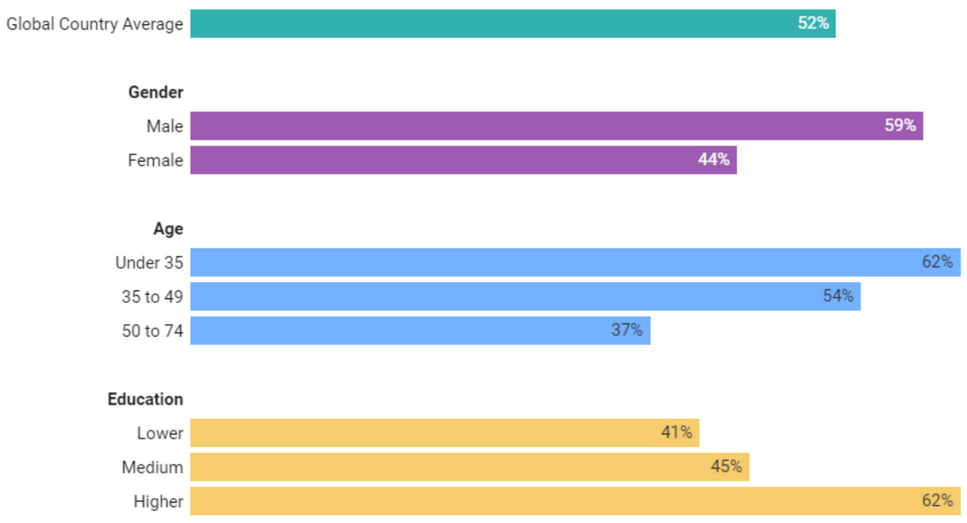


Note. From “Are immersive experiences creating a new digital divide?,” by the World Economic Forum, 2023b, March 8 (https://www.weforum.org/agenda/2023/01/davos23-immersive-experiences-close-digital-divide/).

Another notable division happens along gender identity. The same study shows that globally, regardless of age, men were registered to express greater interest and engagement with Metaverse than women. There are less than half of the female respondents that indicated that they are familiar with Metaverse (Graph 3), and only 34% of women shared that they feel that Metaverse is built for their demographic (*Are Immersive Experiences Creating a New Digital Divide?*, 2023). This is consistent with gender statistics related to the overall digital divide. As of 2022, although women make up close to half of the world's population, only 63% of them were using the Internet compared to the 69% of male users, which is approximately 259 million fewer women with internet access (Facts and Figures 2022 - the Gender Digital Divide, 2022). The same study by the UN specialised agency for the ICTs revealed that the lower-income nations have even more concerning rates of the gender gap with as low as 21% of women having access to cyberspace, compared to 32% of men with internet connectivity, the numbers that have not improved since 2019.

Graph 3

Familiarity across demos: How familiar are you with the Metaverse?[2]



Note. From "How enthusiastic is your country about the rise of the metaverse?," by the World Economic Forum, March 8

[2] Base: 21,005 online adults under the age of 75 across 29 countries, interviewed April 22-May 6, 2022.

(https://www.weforum.org/agenda/2022/05/countries-attitudes-metaverse-augmented-virtual-reality-davos22/).

Another noteworthy difference is that, as one can expect from the high financial barrier to entry, higher income households and the employed population express significantly higher likelihood to engage in Metaverse experiences than lower income households and people who are not actively in the workforce (*Are Immersive Experiences Creating a New Digital Divide?*, 2023). The same study published by the WEF reveals that 49% of those with a household income of $100,000 or higher agree with the statement that the “metaverse is for people like me,” while only 34% of those with household income less than $45,000 think the same. Same research showed that where you live also determines how you feel about the metaverse. The majority of urban residents (59% of those who agree) express personal affinity to the metaverse, while the numbers are lower for the suburban (33%) and rural (36%) residents (*Are Immersive Experiences Creating a New Digital Divide?*, 2023). The reasons behind these differences are yet to be explored.

When opening the discussion on digital divide in Metaverse, it is important to identify who is being excluded from engaging with the virtual reality experiences, as much as it is worthy of asking of who is left behind in designing and shaping the technologies behind the emerging virtual worlds. As has been with the foundation of Web 2.0, this new immersive experiences skew male and Caucasian or Asian developers, all while the global population is 49.58% female and from much more diverse backgrounds (Hardy, 2022). The diversity among the developers is important because it provides a strong point of perspective in considering user experiences that are otherwise neglected.The impact of gender bias in Web 2.0, for instance, is well documented to reinforce societal inequality and shape negative user attitudes in cyberspace (Vlasceanu & Amodio, 2022; Postmes & Spears, 2002). Meanwhile, a research by Gerling & Spiel (2021) revealed that Virtual Reality applications design tends to prioritise an ideal ‘corporeal standard’ and fails to accommodate the needs of special needs alternatives in its research and development (Gerling & Spiel, 2021 as cited in Quinlan, 2023). The study draws an example from Meta’s Oculus VR headsets that are being designed around exclusively normative cognitive, spatial and kinetic capabilities. Considering the scope of impact that Metaverse is projected to create across such industries as healthcare, education, public sector, commerce and others, the implications of negligence to consider experiences and perspectives of some users can lead to dramatic impact on levels of engagement, self-perception and ultimately accessibility of the immersive experiences.

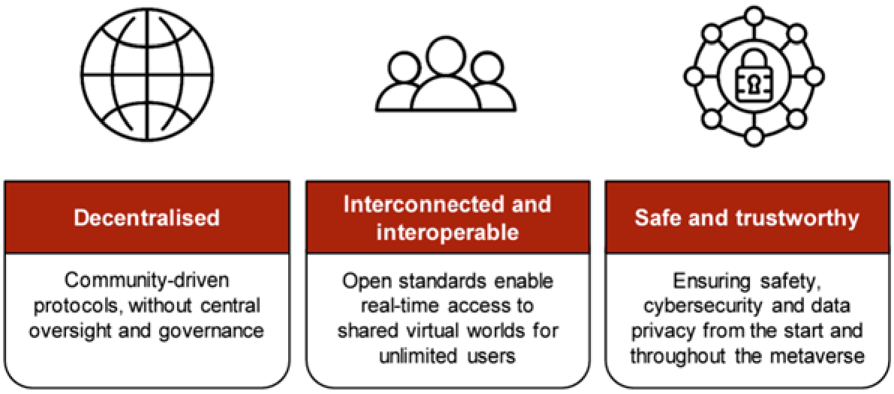
4.1.2 Regulation and Policymaking in Web 3.0

Addressing all of the vulnerabilities discussed in the previous chapter requires a combination of regulatory and policy solutions that can safeguard users and businesses from the potential threats and attacks within the virtual worlds. Nonetheless, at the moment, the Metaverse presents more questions than answers, thereby pressing regulators to grapple with numerous issues. For instance, how will intellectual property generated within a specific metaverse be protected? What taxation policies should be applied to virtual property and land sales? How can instances of sexual harassment or avatar-based harassment be effectively monitored and controlled? How can virtual identities be authenticated? Furthermore, what protocols should be in place for handling healthcare and any other form of personal data in virtual environments? Should each Metaverse world establish its own distinct regulations and standards, and if so, who will be responsible for setting and enforcing these rules? These are just a few of the numerous questions that arise when examining the current state of the Metaverse, and many more questions are not yet imagined as the Metaverse continues to evolve at an accelerated pace in real time.

Although a clear and comprehensive definition and resolution for these regulatory and policy-related questions have yet to emerge, there already exists a general consensus among developers of Metaverse worlds regarding the main principles by which the Metaverse should operate. Those are the principles of decentralisation, interoperability, safety, and trustworthiness (GSMA, 2023, Figure 2). This shared vision can serve as a foundation for initiating a dialogue on the further regulation of the Metaverse. As such, governing the Metaverse presents a complex and multi-faceted challenge that must take into account factors such as interoperability, privacy, cybersecurity, and decentralisation. In the following section, this paper will examine the primary regulatory challenges that are either currently relevant or anticipated in the context of virtual reality.

Figure 2

Key Principles in the Metaverse



Decentralised

Community-driven protocols, without central oversight and governance

Interconnected and interoperable

Open standards enable real-time access to shared virtual worlds for unlimited users

Safe and trustworthy

Ensuring safety, cybersecurity and data privacy from the start and throughout the metaverse

Note. From “The Year Ahead in Digital Policy: Regulating the Metaverse,” by GSMA, *Public Polic*y, January 12, 2023 (https://www.gsma.com/publicpolicy/the-year-ahead-in-digital-policy-regulating-the-metaverse).

Challenges of regulating Metaverse

1. Standardisation and Interoperability

One of the primary defining characteristics of the Metaverse, as well as the broader Web 3.0 Internet, is its decentralised nature. The Metaverse is designed to be independent of any single country or organisation, ensuring that power is shifted away from platform holders and back to the users. Consequently, the infrastructure of the Metaverse operates outside the jurisdiction of any particular country's legislative systems, making it resistant to easy blocking, manipulation, or governance by a singular entity. However, ensuring the effective functioning of the Metaverse presents a significant challenge, particularly in terms of promoting interoperability. ***Interoperability*** refers to the ability of different systems, or virtual worlds in the context of Metaverse, to effectively connect and exchange information with one another (Bates & Samal, 2018).

To achieve this, developers and architects of these Metaverse worlds must collaborate closely to avoid creating closed systems and instead implement common standards that are agreeable to all stakeholders. However, the Metaverse is composed of a diverse array of stakeholders, ranging from major tech companies like Apple, Microsoft, Google, and Meta to national public sector organisations and international entities such as Interpol. This diverse composition can potentially give rise to a collective action problem or social dilemma, wherein all stakeholders would benefit from cooperating with one another based on shared long-term collective interests. However, the conflicting short-term self-interests often hinder joint action, generating a substantial threat that the needed collective benefit may not be realised altogether (Olson, 1965).

2. The dilemma of the distributed governance

The other challenge with decentralisation is that the government, which is usually in charge of outlining policies and regulations in the real world, is no longer in the decision-making seat when it comes to standardisation of the Metaverse. As a result, alternative governance structures are anticipated to emerge, supported by proponents of decentralisation who argue that decision-making authority in the virtual world should reside with users rather than governments or executives. One such alternative structure gaining attention is the ***Decentralised Autonomous Organization (DAO)***.

In one of his articles for CoinTelegraph, the founder and former director of IBM Digital Asset Labs, Nitin Gaur described a DAO as an entity that leverages blockchain technology to document its members, regulations, and obligations on a permanent and unmodifiable ledger. Its constitution and progression are transparent and set in stone. Typically, to become a part of this community, individuals need to invest resources and demonstrate some form of community engagement, usually through the acquisition of tokens, which then allow them to participate or vote in the organisation's affairs (Gaur, 2022). The primary objective of this redefined social organisation is to reduce the influence of intermediaries and representatives. DAOs are envisioned as Web 3.0 user communities that collaboratively work towards a shared vision and adhere to a set of rules enforced through blockchain technology. These communities operate with flat hierarchies, ensuring that each member holds a stake in the DAO without any single individual exerting a "Board of Director"-type control. DAO mechanisms aim to handle governance and economic decisions that impact users within a specific Metaverse world. In theory, DAOs should simply put any moderation and regulation issues for its members to vote on.

While the concept of distributed governance through DAOs appears promising, it lacks a clear mechanism for recourse in cases where governance processes fail or incidents of power abuse occur. In the event that a virtual environment governed by a DAO becomes toxic, the question arises: Who bears responsibility for addressing such issues?

3. Killer acquisitions and ecosystem lock-ins

The discourse surrounding Metaverse regulations encounters an additional challenge in the form of ***killer acquisitions*** that can become prevalent within virtual worlds. The concept of a killer acquisition, as described by Cunningham et al. (2018), refers to instances where big corporations acquire smaller, competitive firms that are engaged in the development of innovative products or services. The primary intent behind such acquisitions is to stifle the progress of these innovative projects and preempt any potential risk of future competition. When building a dialogue on threats and vulnerabilities of regulatory spaces within the virtual worlds, it is important to recognize that the Metaverse is not immune to the risks associated with these predatory practices commonly observed in the realm of big tech. This is because the acquisition of innovative and potentially disruptive companies by larger entities can lead to a consolidation of power, limiting competition, and impeding the development of a diverse and dynamic virtual ecosystem. This may then threaten the very principles of decentralisation, interoperability, and innovation that are crucial to the sustainable growth of the Metaverse.

Another form of killing or rather isolating the competition in Metaverse is Ecosystem lock-ins. ***Ecosystem lock-ins*** may occur when individual world developers leverage their operating systems and underlying technologies to restrict users from accessing products and services created and available within their world in another virtual world. This practice aims to prevent users from transitioning to competing platforms, thereby isolating competition and establishing a dominant market position. Ecosystem lock-ins directly contradict the principles of interoperability that we have previously discussed. Interoperability, which enables seamless connectivity and interaction between different virtual worlds, is essential for creating a cohesive and user-centric Metaverse experience. By erecting barriers that prevent users from freely accessing services across virtual worlds, ecosystem lock-ins would most certainly hinder the realisation of a truly interconnected and open Metaverse ecosystem.

The regulatory challenges associated with ecosystem lock-ins extend to various aspects, including intellectual property rights and responsibilities pertaining to the ownership, control, and processing of the massive amounts of data generated within the Metaverse. As users engage with different virtual worlds, their data is accumulated and stored, raising concerns about data ownership, privacy, and control. Regulating ecosystem lock-ins would require careful and thorough consideration of these issues to ensure that users have full agency over their data and are not subject to unwarranted restrictions imposed by the dominant platform operators.

4. Data compliance and data privacy

The unprecedented amount of personal, biometric and behavioural data that would become available through immersive IOT technologies in the metaverse is one of the key reasons many companies are interested in this space. However, the lack of clear and universally agreed-upon regulations regarding data poses a considerable challenge for regulating the metaverse. Currently, regulatory guidelines and mandates for managing digital data are maintained at the national level, encompassing various aspects such as data acquisition, storage, disclosure, aggregation, analysis, manipulation, use, sharing, selling, and disposal.

However, given that the metaverse exists beyond the confines of a specific physical jurisdiction, it must address the complexities of data flows resulting from geographic constraints. For instance, consider a scenario in which a Kazakh citizen residing in Ireland accesses a metaverse world hosted in China while currently being physically present in Austria. Determining which data laws are applicable to this individual and the experiences they have within different Metaverse worlds becomes a compliance challenge. It raises the question of which laws the platform, data exchange centres, and other stakeholders should prioritise in terms of data handling and protection.

As the metaverse continues to accumulate vast amounts of critical and sensitive data, the implications of data use and data breach extend beyond those encountered in the context of Web 2.0. Thus, the expansion of the metaverse calls for new privacy considerations that address the intricacies of data privacy, data security, and data governance in this unique virtual space environment. Ensuring the protection of Metaverse users' personal information, maintaining data integrity, and safeguarding individuals, businesses and institutions against unauthorised access and misuse of their data become paramount concerns.

5. Transactions and virtual asset ownership

Another significant challenge to regulating virtual space is the decentralised approach to transactions and the establishment of ownership rights within these new Metaverse worlds. The trade of virtual goods opens a wide range of legal considerations that need to be assessed, including issues related to ownership, intellectual property, copyright, trademark, licensing laws, as well as contract, security, tax, and employment law. These legal aspects must be also examined in relation to different crypto currencies, virtual assets, and virtual environments, presenting a broad range of areas that require exploration in the domain of the emerging Metaverse law.

The challenge of the decentralised nature of Metaverse governance, which was addressed in the beginning of this section, gives rise to the challenge of regulating diverse transaction standards and varying virtual ownership rights across different metaverse worlds. Each Metaverse world may develop its own rules and regulations concerning transactions, ownership, and the protection of intellectual property. As a result, users might be put in vulnerable positions having to navigate between these virtual environments where they may encounter inconsistencies, conflicts, and uncertainties regarding their rights and obligations.

In other words, the lack of standardised regulations governing transactions and virtual ownership rights poses a significant challenge for regulating the Metaverse. Without a unified framework, users may face difficulties in understanding and asserting their rights in different Metaverse worlds and different real world jurisdiction systems that might not be up-to-date with a wide array of Metaverse regulations. Additionally, the absence of clear guidelines regarding intellectual property protection and licensing laws in the Metaverse can give rise to disputes and hinder further innovation and creativity within these virtual environments.

4.2 Cross-country Case Studies

Because the discussion regarding the potential challenges and vulnerabilities in the Metaverse is only starting to emerge now, national efforts to regulate virtual space around the world are still in their early stages. Thus, the question of Metaverse adaptation to different state and regional laws remains open. While some countries are proactive in their approach to addressing the vulnerability issues before they arise, others are taking a more cautious wait-and-see approach, leaving the big questions for the market and tech developers to grapple with. Nonetheless, one thing is certain: as the Metaverse continues to expand, legal complexities will arise.

Governments can take action in a variety of ways, such as cooperating with international bodies to establish new legislation, revising existing policies in regards to Web 2.0, and resorting to litigation when necessary. The level of governmental awareness and engagement with the topic might influence the trajectory of

Metaverse development, especially with regards to questions of cybersecurity and data privacy.

The following section of the paper looks at the national case studies of public conversations surrounding the future of virtual worlds and the current landscape of regional initiatives in the Metaverse. With the purpose of presenting the different approaches that states and companies can take regarding the future of the Metaverse, the section specifically looks at the case studies of Asia, the US, and the EU. Each region offers a unique perspective, policies, and regulatory frameworks that reflect their cultural, legal, and technological dynamics at play. Analysing these case studies can contribute to a more comprehensive understanding of the multifaceted nature of Metaverse development, as well as shed light on the potential paths in the evolving landscape of regulating the Metaverse.

4.2.1 The case study of Asia

China

China stands out as a significant player in the development of the Metaverse. According to a report published by the British consulting and analytics firm Globaldata, China is predicted to surpass the West in the level of Metaverse-related investments, solidifying its position as the centre of the Metaverse. The report highlights China's growing emphasis on virtual reality (VR), augmented reality (AR), artificial intelligence (AI), and 6G technologies, which is “aimed to overtake advances in the West and position China as a global hub for the Metaverse" (Globaldata, 2023). Indeed, as of 2021, as many 7000 Chinese companies applied for Metaverse related trademarks, including major tech giants like Tencent, Alibaba, and Baidu that have made substantial investments in the field of Metaverse, exploring various applications (杨希, 2021).

For instance, Alibaba, one of the most prominent players in the Chinese tech industry, has invested €52.8 million in Nreal, a business specialising in augmented reality glasses. Additionally, Alibaba has established an XR laboratory dedicated to researching human-computer interactions, showcasing their commitment to advancing the technological foundations of the Metaverse (Kharpal, 2022). Similarly, Baidu, a renowned internet giant, has introduced a metaverse application called "Xirang," which translates to "The Land of Hope." This app enables users to create digital avatars and explore virtual environments, further contributing to the growing Metaverse ecosystem (Kharpal, 2022; 杨希, 2021).

Furthermore, ByteDance, the parent company of the popular social media platform TikTok, has invested a significant amount of €1.2 billion in the acquisition of Pico, a VR headset manufacturer. It is being predicted that this strategic move positions ByteDance to emerge as a serious competitor to Facebook's Oculus VR division in the XR tech market (Kharpal, 2021). These substantial investments in supporting technologies and research by Chinese tech giants highlight their recognition of the potential of the Metaverse and their commitment to securing the leading position in its global development.

Noteworthy, the investment in associated technologies is not the only strategy that makes China a trend-setter in the Metaverse development. So does the emphasis on expanding the possible applications of Metaverse beyond the dominant fields of gaming, e-commerce and entertainment. In fact, the Chinese Ministry of Industry and Information Technology (MIIT) has published a national-level development plan for the VR sector, emphasising exploration and further integration of virtual reality with industrial applications such as manufacturing (Hui, 2022). The plan sets targets for the establishment of innovative backbone enterprises, pilot cities, and industrial parks to test the integration of XR technologies in sectors like media, education, mining, and even natural disaster management. Chinese provinces and cities, including Shanghai, Beijing, and Zhejiang, have also presented their individual plans to become XR innovation tech hubs, with Shanghai aiming to create a $52 billion Metaverse cluster in the city (Pannone, 2023).

To support Metaverse industries, Shanghai has called for the government to establish special dedicated funds and provide investment subsidies, interest rebates, and other incentives to facilitate further transition to mixed realities. The city administration also highlights that display and processor technology should be advanced further to achieve a better Metaverse immersion experience in the future (Pannone, 2023). Similar initiatives can be observed in other regions, such as Henan province, which has published its own “2022-2025 Metaverse Action Plan” to foster research and innovation.

The overall positive attitude of Chinese businesses and municipalities to actively explore opportunities in Metaverse can be explained by the country's 14th Five-Year Plan (2021-2025). The national plan emphasises the development and strengthening of core industries, including virtual and augmented reality, and identifies specific areas where smart technologies should be applied, such as transportation, manufacturing, education, and medicine (DigiChina, 2022). The collaborative deployment of 5G and IoT is already being observed in China, with instances like the Siming District Court in Xiamen, similarly to Columbia, conducting its first hearing in the Metaverse, with an aim to enhance system transparency and judicial efficiency (PingWest, 2022).

The current state of China's Metaverse development and proactive integration of these efforts in broader national development plans showcases its ambitions to become a global leader in the industry. The country's investments, emphasis on diverse applications beyond gaming and entertainment, and alignment with long-term digitalization strategies also demonstrate its full determination to shape the very future of the Metaverse.

South Korea

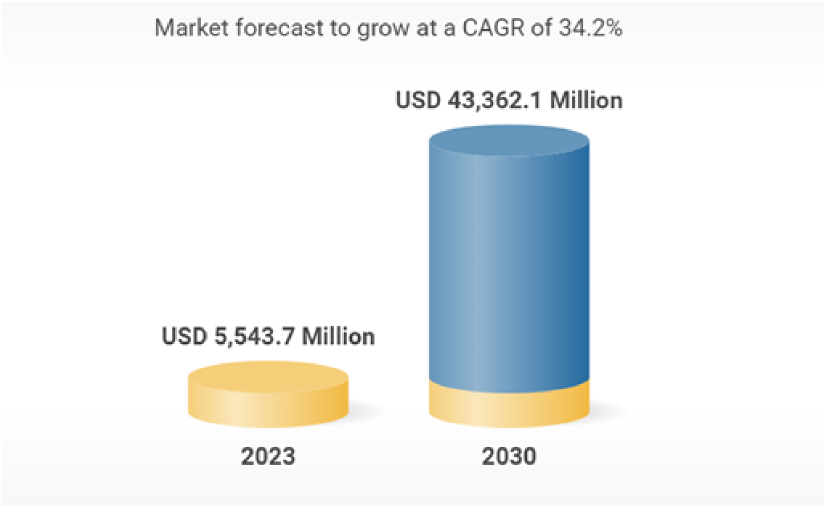
Another prominent actor in Metaverse development is South Korea. Forecasts by the World Economic Forum indicate that by the end of the decade, the country will have the highest penetration rate, reaching 700 million people (*This Chart Shows How Big the Metaverse Market Could Become*, 2023b). Furthermore, a report from the Irish Research and Markets agency predicts a compound annual growth rate (CAGR) of 34.2% for South Korea in the next seven years, with the national Metaverse Spend Value projected to reach US$43,362.1 million by 2030 (Research and Markets, 2023). This upward trend is reflected in the substantial investments made by both major corporations and the South Korean government.

Prominent technology companies such as Naver and SK Telecom, as well as gaming companies like Pearl Abyss, have already recognized the attractive growth potential of the Metaverse and have made significant investments. SK Telecom, a leading mobile operator in Korea, has entered the Metaverse space with its virtual world platform called "Ifland," which has quickly become South Korea's leading metaverse social playground, attracting over 12.8 million cumulative users across 49 countries and 2.6 million monthly active users (*Metaverse Insights in South Korea*, 2023). SK Telecom primarily targets the “MZ generation (Millennials and Generation Z)” through partnerships with diverse players including overseas companies and institutions, such as Danish Birger Christensen that is developing Ifland’s “digital skins” for its avatars to help MZ users express their virtual selves even more (Weissberger, 2022).

Another success story comes from Naver, the South Korean internet conglomerate behind the popular messaging app Line. Naver entered the space of Metaverse with its platform ZEPETO, a mobile-friendly chat application, which allows users to create and interact as 3D avatars in different virtual worlds. Furthermore, ZEPETO allows users to purchase products from renowned brands such as DKNY, Puma, Samsung Electronics, and Marine Serre, which have also established a presence within the virtual world. Notably, ZEPETO has surpassed Ifland in terms of popularity, amassing a user base of over 300 million globally and attracting more than 20 million monthly active users. Impressively, approximately 95% of these users come from international markets, underscoring the platform's widespread global appeal (Weissberger, 2022).

Graph 4

South Korean Metaverse Market



Note. From “South Korea Metaverse Market Intelligence Report 2023: a $43.36 Billion Market by 2030 - Growing Number of South Korean Cities are Seeking a Presence in the Metaverse,” by Research and Markets, *PR Newswire,* May 4, 2023 (https://www.prnewswire.com/news-releases/south-korea-metaverse-market-intelligence-report-2023-a-43-36-billion-market-by-2030---growing-number-of-south-korean-cities-are-seeking-a-presence-in-the-metaverse-301816253.html).

The proactive approach to Metaverse development is not only limited to leading internet and mobile operating companies but also extends to the South Korean government itself. In line with China's goals, South Korea aims to be among the world's leading economies in the Metaverse era. In December 2022, the Metaverse strategy was unveiled by the Ministry of Science and ICT (MSIT), integrated as a key element of the broader Digital New Deal 2.0 initiative. The South Korean government set a national target of becoming the fifth largest country in the global metaverse market by 2026. This will be done by addressing the four main subjects outlined in the Metaverse strategy document (Press Releases - 과학기술정보통신부 >, 2022).

The first is to develop the Metaverse platform ecosystem that fosters core Metaverse technologies and other platforms to grow. The second key element involves bolstering the capabilities of professionals in the Metaverse realm, by expanding business prospects and enhancing access to education within this specific domain. The third pillar is to financially subsidise and incentivise local enterprises specialising in Metaverse to achieve faster international competitiveness; and the fourth pillar outlines the target of making the Metaverse worlds safe and reliable by protecting the community values and eliminating the digital divide in accessing the services within the Metaverse. As noted in the same press release document, while considering the significance of this comprehensive government strategy on Metaverse, remarked that the Metaverse will emerge as a platform where the young generation can embrace more challenges, develop, and advance into a wider world. The Ministry pledged to carry out a multitude of support strategies to affirm South Korea's position as a dominant player in the global Metaverse landscape (Press Releases - 과학기술정보통신부 >, 2022).

Noteworthy, the government acknowledges the importance of developing better regulatory frameworks to ensure safety of the emerging Metaverse worlds and businesses. In February 2022, a partnership agreement, in the form of a Memorandum of Understanding (MoU), was signed between the Ministry of Science and ICT (MSIT) and GSMA, an organisation that represents the interests of mobile operators worldwide. The agreement was made during the Mobile World Congress (MWC) held in Barcelona, with the goal of fostering national and international collaboration on Metaverse strategies. Specifically, the MoU aimed to pinpoint opportunities and challenges associated with Metaverse policies, regulatory standards, and the development of economically viable business models (Press Releases - 과학기술정보통신부 >, 2022). Last year, a significant move towards establishing ethical guidelines for the Metaverse was made by the Ministry of Science and ICT.

They unveiled an ethical framework intended to guide Metaverse developers and users, even though it doesn't carry legal enforceability. This roadmap, termed the "Metaverse Ethical Principles," is the result of cooperative work among a research team of 12 experts from fields including ethics, data protection, law, and engineering. The team's insights were based on the analysis of a survey involving 2,626 respondents, along with other relevant data pertaining to digital safety (Pessarlay, 2022). Consequently, the ethical principles revolve around core tenets of authenticity, fairness, personal data protection, inclusivity, future responsibility, autonomy, and privacy respect.

Not only did the government initiate a conversation on ethical standards that should be explored further as Metaverse expands, but consistent with the second pillar identified in the Metaverse strategy, South Korea also revealed the development of its first “Metaverse Academy.” This program sets the target of training as many as 4,000 national Metaverse and Web 3.0 experts by 2026. As of the moment, the majority of metaverse platforms are available in English. Nevertheless, it has been announced by the Korean government that they plan to construct institutes dedicated to the teaching of the Korean language to non-natives, spanning across various Metaverse platforms. Furthermore, the Metaverse Academy is planned to be leveraged for the international promotion of numerous other Korean sectors, including but not limited to healthcare, arts, K-pop, and tourism.

The Academy will also lure more international talent by helping international Metaverse start-ups to gain entry into the Korean market and become a medium for local content firms. The Ministry of Science and ICT also announced that within the academy framework it will be organising further competitions on Metaverse development and opening hackathons for its students and local start-ups (Muhammad, 2022).

The current state of South Korea's development of the Metaverse demonstrates its clear goals of becoming a global leader in the industry. The government's commitment extends to the establishment of ethical standards, the development of the Metaverse Academy, and fostering international collaboration through partnerships and initiatives. Thus, South Korea's ongoing efforts of both the private sector and the government reflect a clear vision and commitment to harness the potential of the Metaverse for its economic growth and innovation.

JAPAN

By July 2022, Japan's Ministry of Economy, Trade and Industry (METI) also demonstrated its recognition of the significance of Web 3.0 and the advancement of the Metaverse. To solidify this acknowledgment, they established the "Web 3.0 Policy Office" within their existing secretariat (METI, 2022). This office serves as a Cross-Departmental Internal Organization, bringing together various government bodies responsible for Web 3.0 development and facilitating the collection of information from businesses, investors, and legal professionals regarding the challenges faced by Japanese companies in the Web 3.0 environment. The primary objective of this office is to formulate policies related to the Metaverse and its disruptive impact (Pessarlay, 2022a).

The official website of the Ministry highlighted the escalating importance of metaverses as emerging individual environments, specifically among the younger demographic groups such as Generation Z. It also acknowledged the mounting value of digital environments and virtual assets.(METI, 2022). Additionally, the government of Japan acknowledged the concern that local Web 3.0 entrepreneurs are leaving Japan in search of more supportive business environments for their Metaverse ventures. To address this trend, the Ministry emphasised the need to accelerate discussions and strategies on developing a more favourable business environment in Japan. Recognizing the economic impact of entrepreneurs pursuing Web 3.0 - related businesses leaving the country, the Ministry stated its intention to develop up-to-date policies that would deliberate on bills concerning digital assets, decentralised autonomous organisations (DAOs) and the NFTs to foster a more conducive business environment for the Metaverse (METI, 2022).

Similarly to China and South Korea, the establishment of the Web 3.0 Policy Office demonstrates the Japanese government's interest in fostering an environment conducive to Metaverse development. By actively engaging with various stakeholders and formulating metaverse-related policies, the government aims to address the challenges faced by Japanese companies in the Web 3.0 environment and prevent the loss of entrepreneurial talent to overseas markets.

4.2.2 The case of the US

The United States has emerged as a leader in Metaverse and AI development, primarily due to the presence of prominent tech companies located in Silicon Valley. According to Statista, the number of Metaverse users is projected to reach 120.70 million by 2030, with the U.S. currently holding the highest user penetration across global markets at 11.7%, which is expected to grow to 35.5% by the end of the same year (Statista, 2023). This significant market position can be attributed to the active involvement of American tech giants such as Google, Microsoft, Nvidia, Meta Platforms, Roblox Corporation, and Unity Technologies, who have played a vital role in driving AI and extended reality (XR) advancements within American enterprises.

These major players have made substantial investments in Metaverse-related research and development, with Business Insider recognizing Metaverse as the most expensive project in the history of technology (Mann, 2022). Meta, in particular, has invested over $100 billion in Metaverse-focused research and development and an additional $15 billion in product development in the past year alone. In comparison, Sony, a Japanese conglomerate with a significant presence in the video game industry, spends less than $5 billion annually on research and development across all its product lines (Hern, 2022b). Despite these extensive investments, Meta has not yet achieved the desired level of success.

Meta incurred a loss of $13.7 billion in 2022 on its Reality Labs division, responsible for Metaverse expansion, including virtual reality headsets like Quest and virtual environments such as Horizon Worlds (Varanasi, 2023). This underperformance can be attributed to various factors, including a lack of clear strategy, technological limitations, market fragmentation, and intense global competition. Another interesting insight on Meta's performance comes from Celia Pearce, an associate professor specialising in game design at Northeastern University, who voiced her critique of Meta for its inability to nurture user creativity and deliver superior graphics comparable to those that can be found in the gaming sector. In her interview to *Northeaster Global News,* Pearce explained: "Meta really missed the mark in terms of creating something for the right audience. They've also missed the mark in terms of understanding where the industry is, both in terms of what people expect visually from games and what people are actually doing in non-game experiences, which is making stuff. Creativity is the killer app in virtual worlds" (Mello-Klein, 2022).

According to the Brandessence Market Research and Consulting firm, the current U.S. Metaverse Market Trends are adverts in gaming, Web Society, digital assets, a blend of spaces, AI in the Metaverse, crypto in the Metaverse, and the 3D reconstruction (*Metaverse Market Size, Share, Industry Trends Analysis by 2028*, n.d.). And although the U.S. government hasn't made direct investments into the Metaverse industry, it has allocated billions of dollars funding into AI research and development, especially with regards to applying emerging technologies to national security and societal transitions through the new U.S. National Science Foundation (NSF) funded institutions such as the National AI Initiative and seven new National Artificial Intelligence Research Institutes (Nietzel, 2023). The main purpose of their research activities is to find solutions to promoting ethical, trustworthy and resilient AI systems and technologies, investigating new approaches to cybersecurity, expanding our understanding of the human brain, and fostering educational opportunities and public health.

Meanwhile, regarding Metaverse regulation and virtual worlds policy, the U.S. Congress currently adopts a rather passive 'wait and see' approach. Its focus primarily revolves around protecting the competitiveness of U.S. companies in the field and exploring enabling technologies such as AI, blockchain, VR, and AR, rather than considering the broader implications of the Metaverse. Moreover, the absence of federal privacy laws in the United States results in a fragmented and inconsistent legal landscape, with individual state laws often taking precedence. For example, California's privacy laws, lacking enforcement power outside the state, have become the de facto standard (Klosowski, 2021).

Although still in its infancy, the Metaverse industry has already sparked considerable apprehension about regulatory concerns in the United States, specifically in regards to data privacy and safeguarding minors. For instance, last February, few Members of the U.S. Congress shared an open letter to the Federal Trade Commission (FTC), in which they expressed their apprehension about the potential risks that minors might face when accessing different XR products (U.S. Senator Ed Markey of Massachusetts, 2022). In this letter, shared on the official State of the Congress website, they urged the FTC to apply the existing Children's Online Privacy

Protection Act of 1998 and the Federal Trade Commission Act of 1914 in order to safeguard children within the current and future forms of Metaverse.

The authors were particularly worried about the growing trends of VR companies introducing commercial advertisements in the Metaverse. They contended that such practices could have detrimental effects by employing strong marketing strategies targeted at children that can be vulnerable to manipulation and misinformation in virtual environments (Clarke, 2022). Consequently, this joint letter advocated for the United States to implement an up-to-date legislative framework similar to the Age Appropriate Design Code (AADC) introduced in the United Kingdom in 2021. The AADC necessitates that tech companies are restricted with regards to the amount of data that they are allowed to collect from young users, particularly within digital platforms, internet search engines and immersive games that are more likely to be accessed by children and are often driven by the commercial interests (Congress of the United States, 2021).

4.2.2 The case of the EU

According to a recent report published by Research and Markets, the Metaverse businesses present in the European markets are expected to significantly grow in the next decade. The market and research firm predicts that the spend value will reach US$256.6 billion by the year of 2030, demonstrating a staggering annual growth rate of 44.6% (Research and Markets, 2023a). Recognizing this trend, the European Commission has taken a proactive approach to regulate Metaverse development in Europe. Under the "A Europe fit for the Digital Age" program, Commission President Ursula von der Leyen unveiled a new initiative during the State of the Union address. This initiative specifically centres on the Metaverse and its virtual realms, aligning with Europe's overarching goal of achieving technological autonomy by 2030 (Choi, 2023).

This Digital Compass for 2030 acts as a guiding plan to achieve these objectives in virtual worlds and Metaverse development. Its primary focus is to enhance the digital competencies of European citizens and foster experts who can navigate these emerging technological innovations. Furthermore, it seeks to strengthen the European cybersecurity landscape by establishing resilient and self-sufficient data infrastructures independent of third-party entities outside the EU.

Similar to China and South Korea, the European Union has also expressed a clear intention to explore the disruptive potential of the Metaverse as a means to foster economic development and innovation across various industries. In an official statement titled "People, technologies & infrastructure – Europe's plan to thrive in the Metaverse," the European Commissioner Thierry Breton shared a revised Metaverse agenda that outlined the three primary focal areas: "people, technologies, and infrastructure" (Bretton, 2022).

The first focus on people emphasises the need for the emerging Metaverse to be built and ruled around European values with the primary objective of making the environment of virtual worlds be safe for the people. This section also mentions the importance of setting interoperable standards where no private stakeholder has the power to monopolise the industry and solely dictate the terms and conditions for the rest of the Metaverse community. This is promised to be ensured through the string and “future-proof” regulatory frameworks outlined in the European Digital Services Act (DSA) and Digital Markets Act (DMA).

The second focus on technologies highlights the extent to which regulators would be able to shape the Metaverse to make it align with people’s interests will depend on the very ability to develop and master the cutting-edge technologies such as 5G, blockchain, XR sets, HPC and others within the European market.

Thus, Bretton emphasises that it is fundamental to support and invest in the local ecosystem through initiatives such as Virtual and Augmented Reality Industrial Coalition which brings together different actors from the central Metaverse technologies and outlines a roadmap for further development that is approved by over 40 EU organisations (including SMEs, big tech companies and research institutions) that are prominent in this space. Europe is particularly focused on exploring the local development and production of its own energy-efficient and globally competitive semiconductors and hardware, which will be supported by the €6.2 billion of public funds of the new European Chips Act introduced earlier in April this year (*Commission Welcomes Political Agreement on the European Chips Act*, 2023).

The last focus subject outlined by Bretton is the importance of developing a resilient interconnected infrastructure. This comes from the acknowledgement that Metaverse will pose the challenge of unprecedented amounts of big data harvesting and exchange. The new Metaverse worlds will put under even more intense pressure the connectivity infrastructure which is needed to allow all these blockchain developments and crypto and digital payment systems to support the virtual economies. European Commissions, thus, called for making these infrastructures more resilient to disruptions and potential cyberattacks. Furthermore, to tackle vulnerabilities associated with crypto-assets, which are expected to be a vital element in the Metaverse, the European Union took a significant step on April 20th this year. They introduced a pioneering regulatory framework known as the Markets in Crypto-Assets (MiCA) Regulation. This legislation is the world's first and only of its kind, governing the issuance and provision of services related to cryptocurrencies, and sets the EU as the global pace-setter the rest of jurisdictions would contribute to the creation of a safe, robust and necessary ecosystem for crypto asset markets globally,(Banco Bilbao Vizcaya Argentaria, 2023).

In conclusion, while the European Union (EU) has yet to implement specific laws for the Metaverse, both the Commission and Parliament are actively working on a regulatory framework that will be addressing it. This includes initiatives like the 2030 Digital Compass policy program, the European Digital Services Act (DSA), and the Digital Markets Act (DMA). Furthermore, European leaders highlight the significance of equitable and balanced participation from all market participants benefiting from the digital revolution, ensuring fair contributions to public goods, essential services, and infrastructure for the benefit of all the European citizens.

5. Discussion

5.1 Cross-country Comparison

As it was explored in the previous “Cross-national Case Studies” section, the development towards regulation of the Metaverse virtual environments have taken different approaches in the United States, the European Union (EU), and Asian countries. While there are some similarities in the aspirations of creating a safe and resilient virtual landscape, there are also notable differences in their national strategies and the level of engagement with Metaverse.

In the United States, the development of the Metaverse has largely been driven by the dominant private companies and market forces. Tech giants like Facebook (now Meta), Microsoft and Google have invested heavily in virtual reality and augmented reality technologies, envisioning a future where the Metaverse plays a central role in social interactions, digital economy and entertainment. The US approach to driving Metaverse and Web 3.0 transition emphasises innovation, entrepreneurialism, and market competition. Digital environment regulations tend to be more focused on consumer protection, intellectual property rights, and competition policies rather than on explicit control over the type of content or virtual identities. The government also has yet to address how it plans to build regulatory frameworks to handle the cybersecurity concerns that are unique to Metaverse virtual worlds, especially in regards to data harvesting and minors.

In contrast, the European Union has taken a more proactive stance in regulating the Metaverse to safeguard user rights and address ethical concerns. The EU places a strong emphasis on data privacy and protection through the existing General Data Protection Regulation (GDPR) and Digital Service Act (DSA), which sets a well-defined international benchmark for the collection and utilisation of personal data. The EU's approach to the Metaverse also focuses on ensuring fair market competition and preventing the skewed concentration of power by tech giants. Additionally, the EU has shown a commitment to cultural diversity and digital rights, aiming to create a more inclusive and accessible virtual space for all citizens, while actively involving a variety of stakeholders from businesses and industry experts to research institutions.

Meanwhile, Asian countries, particularly China and South Korea, have approached the development and regulation of the Metaverse with a combination of market-driven initiatives and government stimulation. These countries particularly recognize the potential economic and technological benefits of the Metaverse and have made significant investments in virtual reality and gaming industries with a clearly communicated intent of dominating the space of Metaverse in the next decade. In China, there is a stronger emphasis on content regulation and censorship, with the government implementing strict controls over online platforms to maintain social stability and political control. South Korea, on the other hand, has focused on promoting Kpop, gaming and Korean culture, especially targeting the international audience in Metaverse, with policies aimed at fostering the growth of the gaming industry and supporting professional gamers. Meanwhile, Japan is primarily focused on retaining the local talent and providing sufficient infrastructure and other incentives for developers to stay in the local market instead of moving to develop the industry abroad.

While there are overlapping similarities in recognising the role that Metaverse can play in driving future economic prosperity and cross-industry innovation, the approaches taken by the US, the EU, and Asian countries differ in terms of setting priorities, outlining strategies and addressing vulnerability concerns. The US emphasises market competition and innovation, the EU focuses on user rights and ethical considerations, and Asian countries adopt a mix of market-driven and government-led strategies. In other words, it is evident that each country has its own priorities, strategies, and levels of involvement in shaping the direction and regulatory frameworks for the industry.

To understand why that can be the case, this discussion section will now evaluate the results in context of the cross-country comparative framework. In particular, it will look whether the observations regarding each country’s approach to regulating Metaverse are consistent with Kharlamov and Pogrebna’s (2021) ***Human Values-based***

framework for cybersecurity governance. By incorporating this form of comparative cultural analysis, one can gain a comprehensive understanding of the cultural, normative and societal factors that may contribute to the difference in each country’s level of development and regulation of the Metaverse.

5.1.1 The Framework

Numerous studies have highlighted the influential role of a community's underlying values and social norms in shaping their notions of justice and subsequently influencing national attitudes and frameworks regarding regulatory and legal mechanisms (Baldwin et al., 1998; Feather, 1994; Friedman, 1969; Hofstede, 2001; Strelan et al., 2016). For instance, James Allsop, the former Federal Court chief justice of Australia, emphasised the intrinsic connection between law and values. He stated that "Law, at its core, is shaped and influenced by values. These values serve as the basis for a logical and equitable understanding of how power should be structured, utilised, and regulated in both private and public domains. These values manifest not only in legal frameworks but also in societal expectations, behaviours, and actions" (Allsop, 2016). Similarly, research suggests that a group's values also impact their perception of risk, thus influencing their attitudes towards risk control and safety related regulations in particular (Wolff, 2006).

However, there remains a gap in the literature concerning whether the values and norms that influence regulation and safety governance in physical environments also hold significance in cyberspace or virtual environments. Addressing this gap, Kharlamov and Pogrebna (2019) propose a new cross-disciplinary framework that explores the interplay between human values and cyberspace regulation across different countries. Their framework, presented in the paper "Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity," builds upon existing literature in three key domains: community values measurement, regulatory frameworks and the perception of security, and the relationship between community values and security control. By integrating these areas, the authors offer a comprehensive understanding of the interconnectedness between human values and the governance of cyberspace regulation, providing valuable insights into cross-cultural variations in cyberspace regulatory approaches.

Kharlamov and Pogrebna's human values-based framework builds upon Schwartz's theory of cultural value orientations (2006) as its theoretical foundation. Schwartz's theory identifies three main groups of problems that significantly shape human values: the Social problem, Responsibility problem, and Nature problem. The Social problem addresses the coexistence between individuals and the society in which they operate, encompassing the dichotomy of Embeddedness versus Autonomy. The Responsibility problem pertains to the coexistence between individuals and the set of responsibilities within the social fabric in which they operate, involving the tension between Egalitarianism and Hierarchy. The Nature problem explores the coexistence between human groups and larger natural ecosystems, considering the interplay between Harmony and Mastery. By applying Schwartz's framework, Kharlamov and Pogrebna identify two groups of nations: one with more competitive and individualistic value systems, and the other with more cooperative or collective-based systems of values.

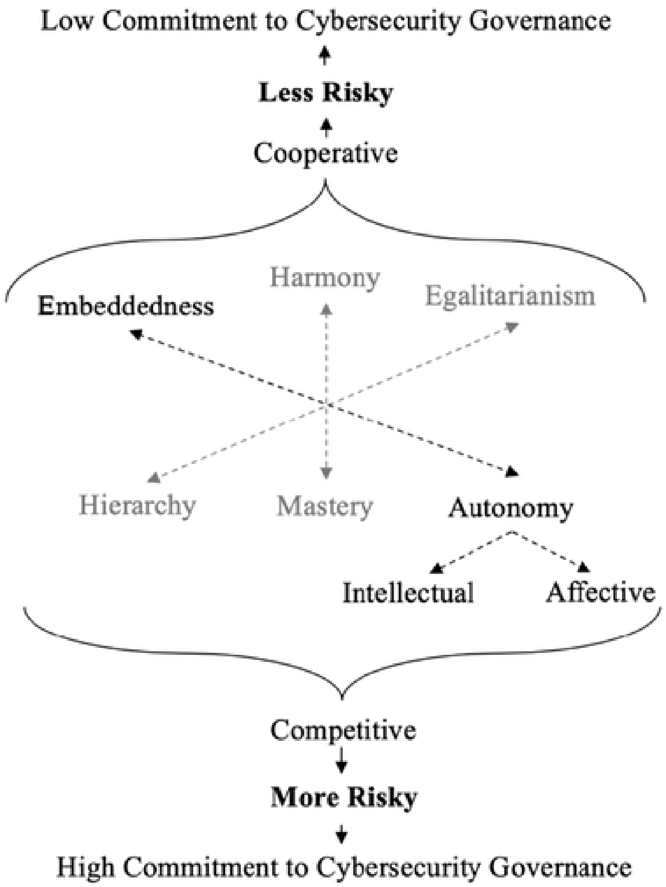
Kharlamov and Pogrebna then identify that in the context of the cybersecurity domain, Embeddedness and Autonomy are the most relevant dichotomies. They argue that the nature and responsibility problems have limited impact in the digital space due to the rarity of hierarchical structures in cyberspace and the fact that people are less likely to consider how their cyberspace behaviour and technologies that allow for that experience influence the natural environment. Consequently, the authors position Embeddedness and Autonomy as the "two major poles of human values" within their framework, with Autonomy being aligned with individual-based values under the Competitive social human values pole, and Embeddedness associated with collective-based human values under the Cooperative system of values pole (Figure 3, Kharlamov and Pogrebna, 2019).

In order to link these poles of cooperative and competitive systems to the issue of cybersecurity, authors then suggest considering the relative propensity of different cultures to engage in risk-taking behaviour within cyberspace. The main assumption that Kharlamov and Pogrebna make through their observations is that one can expect that nations that share more Competitive human values are more prone to engaging into more risk seeking behaviour in all domains, including that of the online environments. Meanwhile, nations that lean towards Cooperative human values systems are more likely to engage in risk averse behaviour in all domains, including that of cyberspace.

The main hypothesis that authors then make based on their refined framework and further research is that as more competitive nations tend to exhibit "riskier" behaviours in cyberspace, these nations then would try to alleviate the potential risks with regards to cybersecurity by building higher levels of cyberspace governance and regulations. At the same time, those nations that share more cooperative values and are less likely to engage in risk-taking behaviour online would then be viewed by their governments as more "self-regulating," and thus would be less engaged on a state level to invest in addressing the cybersecurity problems (Figure 3).

Figure 3

Human values-based framework for cybersecurity regulation



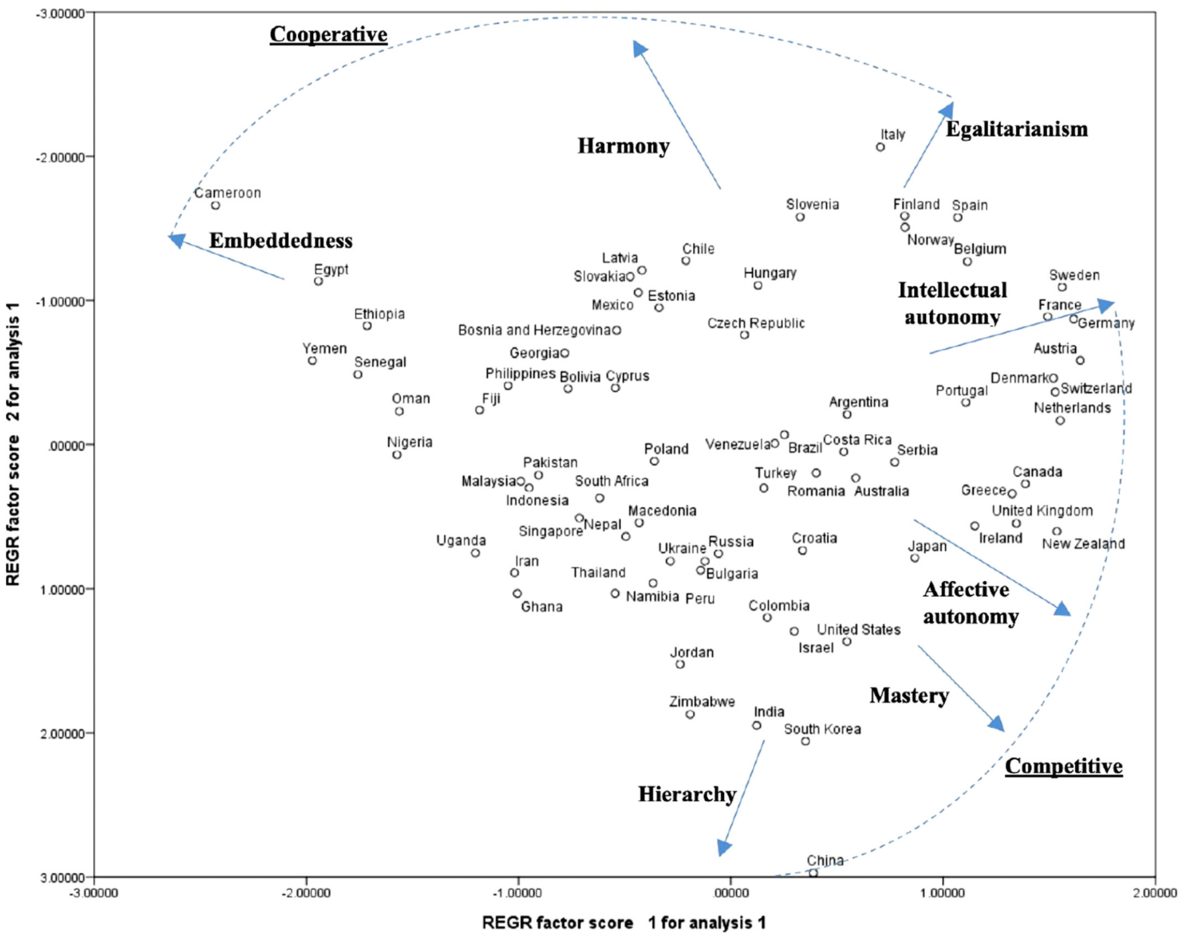
Note. From “Using human values‐based approach to understand cross‐cultural commitment toward regulation and governance of cybersecurity,” by Kharlamov, A., & Pogrebna, G. (2021b). *Regulation & Governance,* 15(3), 709–724 (https://doi.org/10.1111/rego.12281).

5.1.2 Applying the Framework to national case studies

To compare risk attitudes across different cultures, Kharlamov and Pogrebna (2019) apply their new Human Values-based Framework for Cybersecurity Governance to the cross-national dataset collected by Schwartz (2006) for his paper “Basic human values: Theory, measurement, and applications". Schwartz's dataset employed multidimensional scaling to analyse 76 distinct national groups, which were clustered based on seven cultural dichotomies: Embeddedness and Affective or Intellectual Autonomy, Hierarchy and Egalitarianism, as well as Mastery and Harmony. These dichotomies were previously introduced in the "Framework" section above. Kharlamov and Pogrebna then visualise those seven dimensions along the two poles of Cooperative versus Competitive cultures (Graph 5).

Graph 5

The seven dimensions of the Cooperative versus Competitive cultures



Note. From "Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity," by Kharlamov, A., & Pogrebna, G. (2021b). *Regulation & Governance,* 15(3), 709–724 (https://doi.org/10.1111/rego.12281).

Graph 5 demonstrates that, according to Kharlamov and Pogrebna framework of value orientations, South Korea and China are positioned relatively nearer to the Competitive values end (located at the lower right corner of graph 5) in comparison to the United States, which is still placed closer to the Competitive group in comparison to Japan. Nonetheless, both Japan and other Asian countries, along with the United States, display a higher inclination towards Competitive values when compared to the United Kingdom and the majority of European countries, including the Netherlands, Denmark, Austria, Portugal, and Germany.

Therefore, according to Kharlamov and Pogrebna's framework, Chinese and South Korean citizens are expected to be relatively more inclined to make riskier decisions compared to Americans. Similarly, Americans are predicted to have a higher propensity for risk-taking than the Japanese, who, in turn, are more likely to make riskier decisions compared to most Europeans. The authors validate this framework of risk-taking tendencies by referencing previous studies that demonstrated a parallel pattern in the context of online environments. These studies indicated that Chinese individuals are more prone to taking risks in online environments than most Americans, while Americans exhibit a higher likelihood of online risk-taking compared to those from the UK (Pogrebna and Skilton, 2019; Kharlamov et al., 2018). By highlighting these empirical findings, Kharlamov and Pogrebna provide supporting evidence to advocate for their framework's alignment of the cross-national real-world risk-taking inclinations and the risk-taking behavioural patterns in cyberspace.

As discussed earlier in the "Framework" section, Embeddedness and Autonomy are identified as particularly relevant dichotomies in cyberspace. The authors suggest that countries with higher scores along the Affective or Intellectual Autonomy lines are more likely to be proactive and effective in regulating cyberspace. This is because governments in such countries recognize the need to prevent the potentially negative impact of higher rates of online risk-taking behaviour among their citizens. In fact, the authors state that “in such Competitive nations, individuals will not view their rights in cyberspace (such as, e.g. the right to privacy or personal data protection) as inherent human rights due to the individual-based and more challenge-oriented nature of the value system…Such behaviour will generate risks which, in turn, would need a more effective and precise regulation” (Kharlamov and Pogrebna, 2019). On the other hand, countries that exhibit higher cooperative values, such as the European Union compared to the US and Asia (as shown in Graph 5), are regarded as countries that rely less on governing cyberspaces efficiently through regulation, as they anticipate alternative societal mechanisms to fulfil that role (Kharlamov and Pogrebna, 2019).

Thus, when applying Kharlamov and Pogrebna's Human values-based framework for cybersecurity regulation to the context of national regulations in the Metaverse, it can be predicted that cultures driven by Competitive values, such as China, South Korea, and the United States (as shown in Graph 5), will be more efficient and proactive in establishing cybersecurity regulations within virtual worlds. On the other hand, cultures driven by Cooperative values, like Japan and the European Union, are expected to be less interested and less efficient in governing the Metaverse. This is because these cooperative-oriented nations rely on alternative mechanisms beyond strict regulation to address the challenges of cyberspace.

However, this proposition does not fully align with the current regulatory trends discussed in the "Cross-country Comparative Section" of this paper. Despite China's proactive attitudes towards regulating the Metaverse, the government primarily focuses on subsidising the industry and expanding Metaverse applications in various sectors, such as urban environments, education, and the public sector. There have been no public discussions or policy drafts addressing cybersecurity, data privacy, or other user vulnerabilities in virtual environments. Similarly, the United States, which is expected to have more efficient regulations concerning online security concerns, lacks comprehensive federal privacy laws related to online data privacy, with the last Privacy Act being established in 1974. The case of a U.S Congressman's letter to the Federal Trade Commission appealing for the protection of children's data in cyberspace further highlights the gap in American cybersecurity governance.

However, contrary to what Kharlamov and Pogrebna's framework would predict, the governance efforts related to the Metaverse show that the European Union does not adopt a more passive stance on cybersecurity issues compared to the United States or Asia. On the contrary, recent developments such as the 2030 Digital Compass agenda, "A Europe fit for the Digital Age" program, and the Digital Service Act demonstrate proactive involvement of European states in regulatory efforts concerning vulnerabilities in data protection, big tech monopolisation, and Metaverse-related regulations. This observation indicates that although Chinese and American online users may engage in riskier behaviours compared to European internet users, their governments' responses to protecting people's security in cyberspace do not necessarily align with these behaviours. The reasons for this discrepancy may vary and require further empirical research and exploration.

5.2 Main Vulnerabilities

Upon examining the findings outlined in the Results section of this study, it becomes evident that the Metaverse offers significant potential across a wide range of cross-industry applications. However, this potential is not without challenges, as the Metaverse also presents notable concerns, specifically regarding potential risks and vulnerabilities, including identity theft, cyber attacks, disinformation, virtual exclusion, and privacy issues. Within the Metaverse's framework, users are afforded the ability to fabricate virtual avatars that can be strikingly similar to their real-life selves, which could potentially be exploited for deep fakes and fraudulent impersonations. This can result in impersonation, financial fraud, disinformation and other criminal activities.

Consider, for instance, the criminal usage of these fraudulent avatars to compromise user accounts, illicitly acquire personal information, or conduct fraudulent transactions. The likelihood of using these deceptive avatars to also harass or intimidate other users cannot be overlooked. Therefore, it becomes imperative for users to exercise caution regarding the information that they disclose in the first place and to remain vigilant for signs of identity theft and fraud, as well as to actively report dubious activities to the relevant moderators or regulatory systems.

The Metaverse, given its complex and interconnected nature, is also susceptible to cyber attacks. As a result, potential disruptions to the Metaverse, theft of user data, or even physical harm to users due to hacking of VR, AR or any other wearable technologies are plausible outcomes. Hypothetically, hackers may exploit vulnerabilities in the Metaverse's hardware or software to infiltrate user and business accounts.

The more businesses and organisations move to the Metaworlds, the higher is the risk that unaddressed privacy risks can lead to disrupting the physical world operations. The additional layer of threat also comes from the fact that due to the IOT nature of the Metaverse, users will inevitably share an increasing amount of personal data with the entities that create and operate these platforms. Additionally, without proper measurements in place, users can become vulnerable to losing not only their personal data, but also their unique and unchangeable biometric data such as blood pressure, eye tracking, breathing patterns, among others.

The resulting data could potentially be exploited to track the users, target them with tailored advertising, or even manipulate their political decisions by creating virtual world echo chambers. Therefore, commercialization of personal data as it is a common practice among social media companies today must undergo a more vigorous management within the Metaverse to safeguard biometric and other personal data effectively, and employ ethical transparency regarding the way users' personal data is managed. Moreover, it is incumbent upon the Metaverse infrastructure developers to deploy stringent security measures and collaborate with law enforcement agencies to investigate, prosecute, and prevent virtual worlds' cyber attacks. It is also crucial for users to have a full comprehension of how their data is being collected, processed, and utilised, and be reminded to remain cautious about the information they disclose within the Metaverse.

These security and privacy risks associated with the Metaverse are being acknowledged by all of the nations discussed in this paper, as illustrated in the case studies. Noteworthy, initiatives include formation of special industry stakeholder groups conducting a more in depth research on potential vulnerabilities, and consideration of new governing regulations. However, while countries started recognising potential data and privacy vulnerabilities of virtual environments, there has yet to come a public discussion on building solutions to address the issue of virtual deepfakes, disinformation, virtual divide and exclusion, as well as the overall rule of law in Metaverse. It is also vital to acknowledge that not all risks can be mitigated solely through policy and regulation; some risks necessitate technical solutions. For instance, Metaverse technology developers must implement robust blockchain security measures to safeguard user data. In order to make those solutions sustainable, a thorough understanding of all the affected vulnerability groups must be considered. In addition, the diversity and inclusion in the space of developers must be prioritised to ensure a complete and holistic approach to secure a safe space for all the participants.

Therefore, based on the Metaverse vulnerability assessment, this paper identifies three areas for threat mitigation:

1. **User Education**: One of the most effective strategies for mitigating the security and privacy risks in the metaverse is user education. Awareness about the potential threats of sharing personal data in the metaverse, coupled with knowledge about the available protective measures, is crucial.

2. **Technical Solutions**: As previously discussed, certain risks demand technical solutions. Metaverse technology developers must incorporate stringent security measures to safeguard user data, such as employing robust encryption, implementing rigorous authentication procedures, and actively monitoring for suspicious activities.

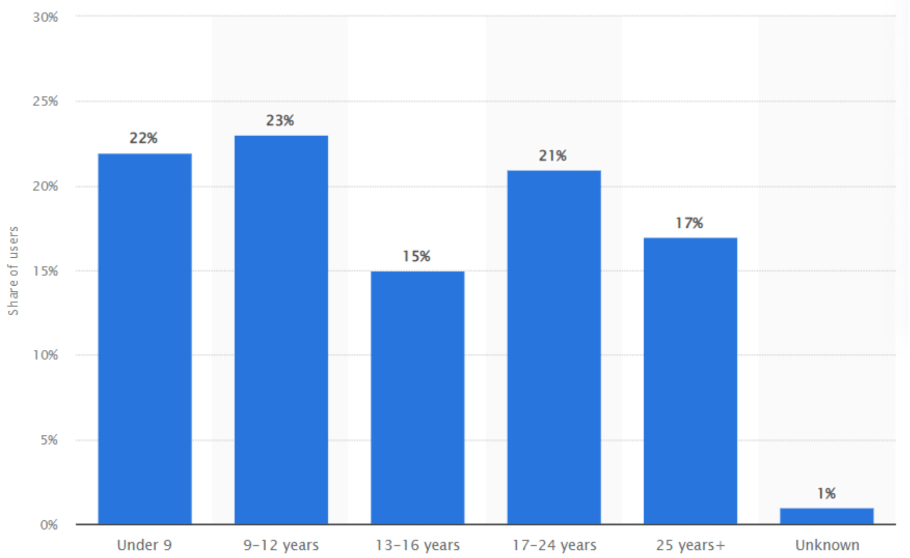
3. **Government Regulation**: Government and transnational regulatory intervention can also play a significant role in mitigating these risks. Legislative measures regulating data collection and usage within the metaverse, coupled with the establishment of enforcement agencies, can significantly enhance the safety and security of virtual environments.

5.3 Main Vulnerability Groups

When evaluating the inherent vulnerabilities found within the Metaverse, it is also imperative to carefully consider those social groups that may be disproportionately susceptible to such risks. At the moment, Metaverse worlds are predominantly concentrated within the realms of gaming and entertainment with a considerable portion of its content being specifically designed to captivate younger demographics. An example of this is Roblox. Being one of the most universally popular Metaverse worlds, Roblox currently attracts 66.1 million daily active users and over 214 million monthly active users (Ruby, 2023b). Backlinko reports that 67% of those users are under the age of 16 (Dean, 2023). In fact, as of 2020, according to Roblox Investor Day presentation, as high as 45% of Roblox's daily active users have not even reached the age of 13 (Graph 5).

Graph 6

Age distribution of Roblox's user base, as of December 2022



Note. From "Global Roblox game user distribution by age 2022," by Statista, April 19, 2023 (https://www.statista.com/statistics/1190869/roblox-games-users-global-distribution-age/).

Nonetheless, there hasn't been enough acknowledgement of how the risks in Metaverse might differ when being experienced by minors, as well as the impact of experiencing mixed reality environments as a child. Majority of traditional literature focuses on cyberspace experiences of adults. Additionally, there is a lack of understanding of how the unique characteristics of embodied internet and sharing of virtual environments with adults impacts underaged users. Hence, it is not merely sufficient to identify and comprehend the vulnerabilities and threats within the Metaverse; but it is also equally important to raise a discussion on the most vulnerable user demographics and unique characteristics of their user experiences in virtual worlds. Specifically focusing on potentially vulnerable groups can then allow for the development of more tailored and comprehensive protective strategies and safety regulations.

5.3.1 Minors

On April 14, 2023, a collective of almost seventy child protection advocates, led by organisations as Fairplay, the Center for Digital Democracy (CDD), and the Center for Countering Digital Hate (CCDH), directed a letter to Mark Zuckerberg, Meta's CEO. The letter appealed to him to reconsider the decision to permit minors into their Metaverse application, Horizon Worlds. As covered by Bloomberg, these advocacy groups urged Meta to conduct an exhaustive examination of the potential risks associated with granting children access to the Metaverse, considering the high likelihood of their exposure to harassment and breaches of privacy in these virtual environments (Birnbaum, 2023).

This shared concern was substantiated by empirical evidence collected by the Center for Countering Digital Hate, as detailed in their report from March of the current year. In this publication, advocates documented multiple instances of harassment and age-inappropriate content directed at users below the age of 18 during their review of the Horizon Worlds. This harassment encompassed a spectrum from sexually explicit insults to expressions of misogyny, homophobia, and racism (Center for Countering Digital Hate, 2023).

Corresponding observations were also put forth by various investigators, such as Catherine Allen from Limina Immersive, Jess Sherwood, a researcher at the BBC, and independent producer Rachel Seifert. During the compilation of a report on virtual reality for the Institute of Engineering and Technology, Catherine Allen acknowledged that while many of her virtual reality encounters were thrilling and enjoyable, certain interactions were undoubtedly traumatic and unsettling (Crawfard and Smith, 2022). She recounted an event in Meta's Horizon World where she was compelled to step in and shield a seven-year-old girl from a group of men who circled her and "joked about raping" directed at both of them. Reflecting on the incident in an interview with the BBC, Ms. Allen shared: "I shouldn't have had to do that, but that's because there's no moderation, or apparently very little moderation" (Crawfard and Smith, 2022).

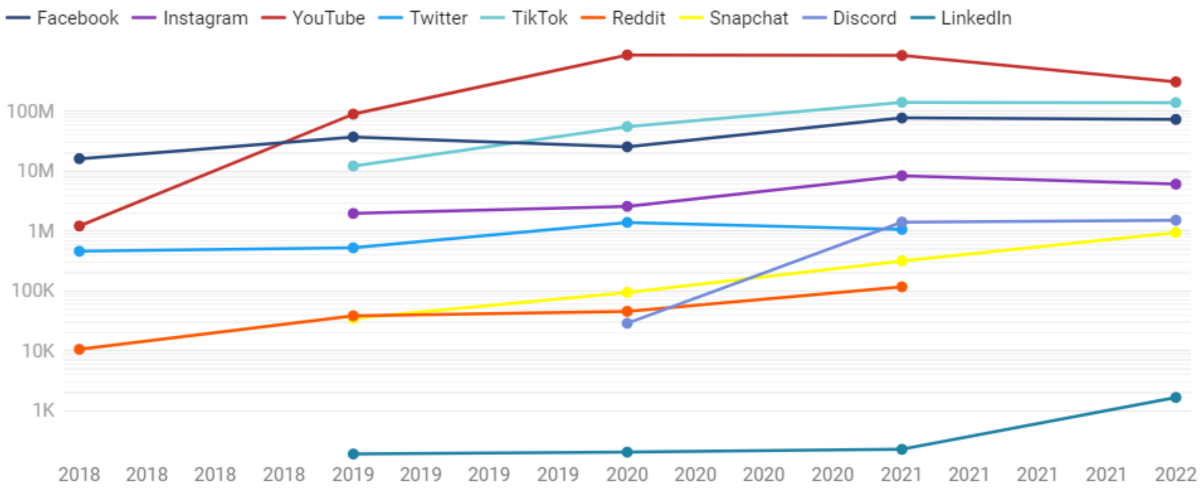
Jess Sherwood, a researcher from BBC, echoed these disturbing observations drawn from her own social experiment wherein she assumed the persona of a 13-year-old girl within Meta's Horizon World. There, she was exposed to inappropriate content for her assumed age, endured sexual and racial slurs, and was subjected to explicit threats of sexual violence (Crawfard and Smith, 2022). Concurrently, Callum Hood, who leads research at the Center for Countering Digital Hate, embarked on an independent study involving the documentation of his virtual interactions on VRChat over a multi-week period. Within a single duration of 11 hours, Hood reported witnessing in excess of 100 worrisome incidents on VRChat, some of which involved users who shared to be below the age of 13. He similarly reported instances of sexual and violent threats against minors and exposure of minors to sexually explicit content. Hood critiqued the VRChat developers and Meta for failing to implement adequate protective measures in virtual environments of their Metaverse worlds, thereby creating an environment conducive to abusive users and highly unsafe for minor users (Frenkel & Browning, 2021).

Unfortunately, the concerns regarding the safety of minors in online environments are not novel for Meta. The alarming patterns of sexual harassment in the virtual reality of Metaverse worlds only mirror the existing threats and risks encountered by children within Web 2.0 platforms. Between the first and third quarter of 2022 alone, Meta identified an astonishing 73.3 million instances of content that fell under the category of "child nudity and sexual exploitation" on Facebook. This figure is just 4 million short of the total of 77.5 million similar reports that were recorded in 2021. These disconcerting statistics were provided by Bishoff and Moody (2023) who highlight that Facebook is not alone in its failure to eliminate content involving child abuse. Other platforms, including Instagram, Youtube, Twitter, TikTok, Reddit, Snapchat, Discord, and even LinkedIn collectively remove millions of posts and images that go against the community standards concerning child safety and abuse (Bischoff & Moody, 2023; Graph 7).

Graph 7

Social media content and account removals for child abuse and safety - 2018 to Q3 2022[3]

[3] Data unavailable for 2022 for Twitter and Reddit. Facebook, Instagram, YouTube, TikTok, and Discord data for Q1-Q3 of 2021. Snapchat and LinkedIn data for Q1 and Q2 of 2021. YouTube data



Note. From “The rising tide of child abuse content on social media,” by Bischoff, P., & Moody, R., *Comparitech,* 2023 (*https://www.comparitech.com/blog/vpn-privacy/child-abuse-online-statistics/*).

Children are not merely disproportionately susceptible to harassment in digital spaces, but they are also disproportionately exposed to abuse based on their geographical location. Bischoff and Moody (2023) cite a report from the National Center for Missing & Exploited Children, delineating the top ten nations for online child exploitation material. Topping the list is India, with 4,699,515 reported instances and a dramatic 73% escalation in referrals compared to 2020. Subsequent to India is Pakistan, with over 2 million annual cases and a 58% increase in reports since 2020, followed by Indonesia and Bangladesh, observing alarming increases in reported child abuse materials by 89% and 113% respectively.

Several of the top ten countries, such as Iraq, Vietnam, and Bangladesh, suffer from lack of sufficient legislation or coherent procedures to counter online child pornography. For instance, Bangladesh's Digital Security Act entirely disregards and fails to address online child abuse (Survey Finds 30% Children Were Abused Online During Pandemic, 2021). Furthermore, when such cybercrimes are seldomly

combined: content, comments, and accounts. Twitter data combined: content and accounts. Discord data combined: content, accounts, and servers.

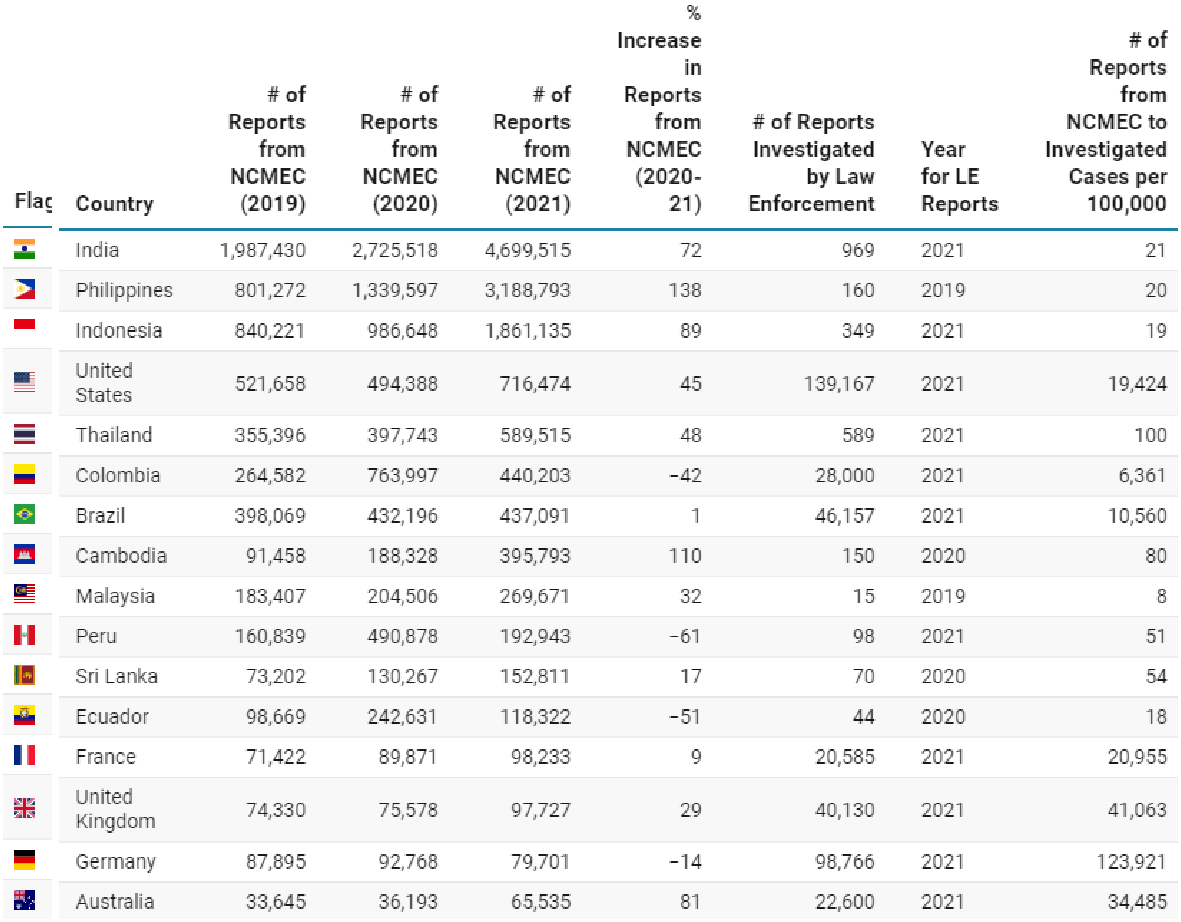
addressed, there exists a discernible void in local infrastructure and competencies to appropriately investigate these cases.

It is particularly worrying that the number of investigated cases of online abuse and harassment targeting underaged internet users is significantly inadequate in Asian countries. Nonetheless, this failure to safeguard the most vulnerable group in cyberspace is still a universal shortfall. According to Bischoff and Moody (2023), across the globe, only 3,467 cases for each 100,000 of reports were investigated further. Noteworthy efforts to fight this issue were made by Germany, France, and the UK (Table 4). This proactive approach to regulating cyberspace and ensuring the safety of online and virtual environment platforms aligns with the observations made in the cross-country comparative analysis section of this research.

The European Union, unlike Asia and the US, currently leads the discourse on addressing vulnerabilities and potential threats that might be reintroduced in Web 3.0. It is also worth noting that Bischoff and Moody observe a decline in the US's proactivity to investigate reported internet crimes against minors by law enforcement, which underscores the concerns expressed by the U.S. Congress members in their letter to the Federal Trade Commission (FTC), as discussed earlier in the US case study section of this paper.

Table 4

The number of Reports made from NCMEC to Investigate Online Child Abuse Cases



Flag	Country	# of Reports from NCMEC (2019)	# of Reports from NCMEC (2020)	# of Reports from NCMEC (2021)	% Increase in Reports from NCMEC (2020-21)	# of Reports Investigated by Law Enforcement	Year for LE Reports	# of Reports from NCMEC to Investigated Cases per 100,000
🇮🇳	India	1,987,430	2,725,518	4,699,515	72	969	2021	21
🇵🇭	Philippines	801,272	1,339,597	3,188,793	138	160	2019	20
🇮🇩	Indonesia	840,221	986,648	1,861,135	89	349	2021	19
🇺🇸	United States	521,658	494,388	716,474	45	139,167	2021	19,424
🇹🇭	Thailand	355,396	397,743	589,515	48	589	2021	100
🇨🇴	Colombia	264,582	763,997	440,203	-42	28,000	2021	6,361
🇧🇷	Brazil	398,069	432,196	437,091	1	46,157	2021	10,560
🇰🇭	Cambodia	91,458	188,328	395,793	110	150	2020	80
🇲🇾	Malaysia	183,407	204,506	269,671	32	15	2019	8
🇵🇪	Peru	160,839	490,878	192,943	-61	98	2021	51
🇱🇰	Sri Lanka	73,202	130,267	152,811	17	70	2020	54
🇪🇨	Ecuador	98,669	242,631	118,322	-51	44	2020	18
🇫🇷	France	71,422	89,871	98,233	9	20,585	2021	20,955
🇬🇧	United Kingdom	74,330	75,578	97,727	29	40,130	2021	41,063
🇩🇪	Germany	87,895	92,768	79,701	-14	98,766	2021	123,921
🇦🇺	Australia	33,645	36,193	65,535	81	22,600	2021	34,485

Note. From “The rising tide of child abuse content on social media,” by Bischoff, P., & Moody, R., *Comparitech,* 2023 (https://www.comparitech.com/blog/vpn-privacy/child-abuse-online-statistics/).

This is to show that the concerns raised by children’s rights activists in regards to the vulnerabilities prevalent in Metaverse realms are firmly rooted in the grim present-day trends of criminal offences perpetrated against minors in today’s internet space. As the Metaverse continues to expand, the protection of children, who may become the pioneering generation to grow up within the augmented realities with an amplified presence in virtual domains, calls for a very thoughtful consideration. The anonymous nature of virtual avatars and the absence of physical evidence can make it increasingly challenging to identify and protect children from potential perpetrators. Meanwhile, virtual reality harassment could potentially be more traumatising than harassment and bullying presently encountered in cyberspace. This is given the immersive, all-embracing mixed reality experiences facilitated by virtual environments, in which unwanted touch can be made to feel as real and fully sensory as when experienced in real life.

It’s fundamental for both children and their parents to secure confidentiality of their personal data. It is also crucial for users to become fully cognizant of the potential dangers inherent in engaging with anonymous or unknown entities in virtual worlds. It is also equally essential to establish a clear and easy to use reporting system for children to report any suspect or inappropriate behaviour. Ultimately, the formulation of up to date policies and guidelines to address the inappropriate behaviour in the Metaverse is required, along with an overhaul of national legal frameworks and procedures to scrutinize any instances of child abuse within mixed realities. In conclusion, the experiences shared by numerous researchers, advocates, and users should serve as an urgent call to action, demanding a development of deliberate and robust approach towards shaping the future of the Metaverse that acknowledges and addresses the vulnerabilities and risks encountered by its disproportionately large percentage of underaged users.

It is also worth reflecting how our current cyberspace realities reflect the way existing mechanisms fall short of protecting the most vulnerable among us. As countries around the world make a shift into a new era of the Internet, the failures and lessons from Web 2.0 need to set the foundation for informing development of a more ethically grounded Web 3.0. The Metaverse should not replicate or exacerbate the failings of our current digital world, but rather, it should strive to correct them.

6. Conclusion

6.1 Summary

The purpose of this study was to investigate the regulatory challenges and high-risk implications of the emerging Metaverse, with a specific focus on cross-country comparisons, the role of tech giants, and the vulnerabilities faced by users. The goal was achieved through the mixed-methods approach, which incorporated a thorough literature review, a cross-country comparative analysis, and the inclusion of secondary empirical evidence from journalistic reports and scholarly studies.

The cross-country comparison revealed distinct approaches to fostering and regulating the Metaverse. The United States emphasised innovation, entrepreneurialism, and market competition, with dominant tech companies driving the development. Contrary to that, the European Union took a more proactive stance to ensure the safety of user rights, address ethical concerns, and protect fair market competition. Asian countries, on the other hand, particularly China and South Korea, adopted a combination of market-driven initiatives and government stimulation, aiming mainly at the goal to dominate the global Metaverse industry.

These findings then were evaluated against Kharlamov and Pogrebna's Human Values-based Framework for Cybersecurity Governance, which identified cultural values as influential factors in regulating cyberspace. As this study finds, there were discrepancies between the framework's predictions and the regulatory trends observed in the case studies. The European Union, despite exhibiting more cooperative values, demonstrated proactive efforts in addressing vulnerabilities, while the US and Asia, with more competitive values, had mixed responses.

The role of multinational tech giants, such as Meta, Microsoft, and Google was also found to be significant when shaping the development of the Metaverse. These companies invested heavily in virtual reality and augmented reality technologies, envisioning a future where the Metaverse plays a central role in not only social interactions, but also the digital economy, and entertainment landscape. However, the influence of these companies raises concerns about data privacy, content regulation, and the concentration of power. The issue of the digital divide and social exclusion was also evaluated in the Finding section of the paper. Furthermore, the regulatory challenges associated with data compliance and data privacy in the Metaverse were discussed. The decentralised nature of the Metaverse was found to pose complexities in determining applicable data laws across different jurisdictions.

The vulnerabilities faced by minors in the Metaverse emerged as another critical concern in evaluating the vulnerability groups in this discourse. Journalistic reports and studies highlighted instances of harassment, age-inappropriate content, and threats directed at underage users. Noteworthy, the safety of minors in virtual environments mirrors the existing risks encountered in Web 2.0 platforms. The anonymous nature of virtual avatars and the immersive experiences in the Metaverse create significant challenges in identifying and protecting children from potential perpetrators, highlighting the need for improved safety measures and protection for underage users.

6.2 Limitations

While this research provides valuable insights into the regulation and vulnerabilities of the Metaverse, there are some limitations to consider. Firstly, the rapidly evolving nature of the Metaverse presents a challenge as new information emerges in real-time, and a significant portion of the available sources are directly from developers, user-based forums or journalistic works. There is a scarcity of empirical research and academic literature that specifically focuses on real-time trends and emerging risks identified in this paper. This limitation still highlights the need for further research which would fill in these gaps, and extend a more up-to-date understanding of the evolving Metaverse landscape.

Secondly, working with different country case studies, especially within the Asian context, introduced limitations due to the availability of information in English. While efforts were made to gather data from official ministry statements and reputable sources, the language barrier may have resulted in potential information gaps or nuances being overlooked. As a result, further studies that would encompass a wider range of languages and extend the perspectives from non-English-speaking countries would contribute to a more comprehensive analysis of the global trends in development and variety of regulatory approaches.

6.3 Future Directions

Further research might be needed to look deeper into the cultural, normative, and societal factors that shape Metaverse regulation. Additionally, more empirical studies would be needed to look into the user experiences of different social groups, especially the minors. The overall effectiveness of current or near-future regulatory measures must also be accessed further.

Other research directions may also consider the challenges of distributed governance in the Metaverse, different mechanisms for addressing killer acquisitions and ecosystem lock-ins, data compliance and privacy regulations across jurisdictions, and the establishment of standardised ownership rights.

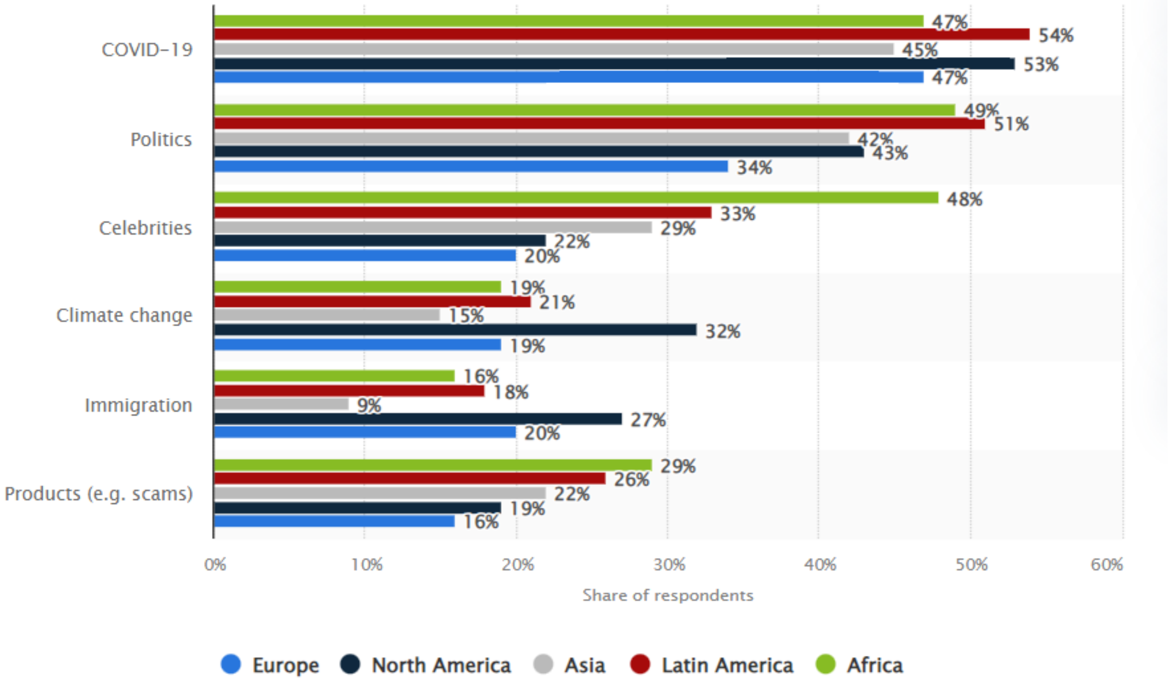
Last but not least, it is important to evaluate what psychological implications Metaverse has on its users. This should include an outlook on the potential impacts on mental health, social interactions, and identity formation for minors who grow up inside of Metaverse. This would further contribute to a more holistic understanding of this emerging virtual and mixed-reality landscape.

In conclusion, this research highlights the complex risks and regulatory challenges together with potential implications surrounding the growth of the Metaverse. It underscores the necessity for a comprehensive and collaborative multi-stakeholder approach that would involve policymakers, tech companies, advocacy groups, parents, and users themselves to ensure the privacy and well-being of new Meta World residents. Addressing the identified vulnerabilities and regulatory gaps can become the first step in shaping a more ethically grounded Web 3.0 that faces the shortcomings of the current digital world while fostering a safer experience of the Metaverse.

Tables and Graphs

Graph 1

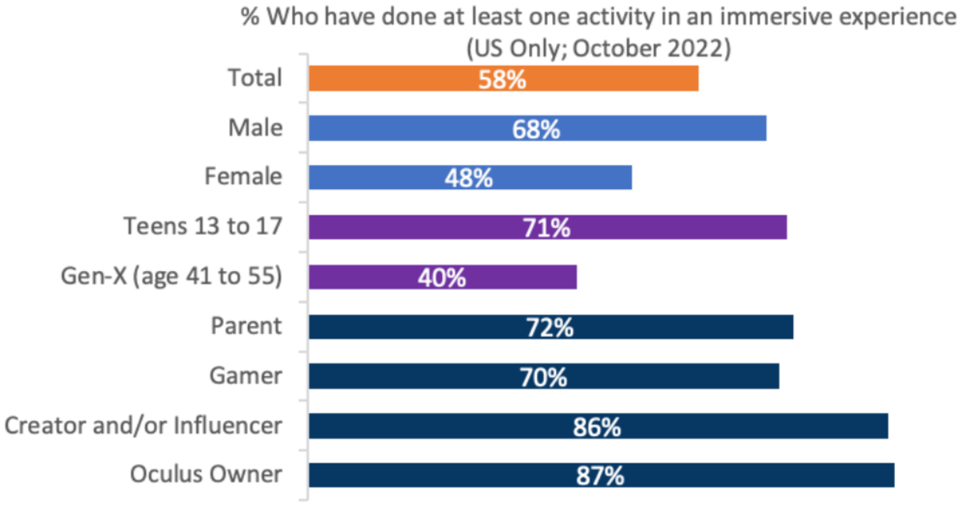
News consumers who saw false or misleading information about selected topics in the last week worldwide as of February 2022, by region



Note. From “Consumers witnessing false information on certain topics worldwide 2022, by regions,” by Statista, 2022b, June 28 (https://www.statista.com/statistics/1317019/false-information-topics-worldwide/).

Graph 2

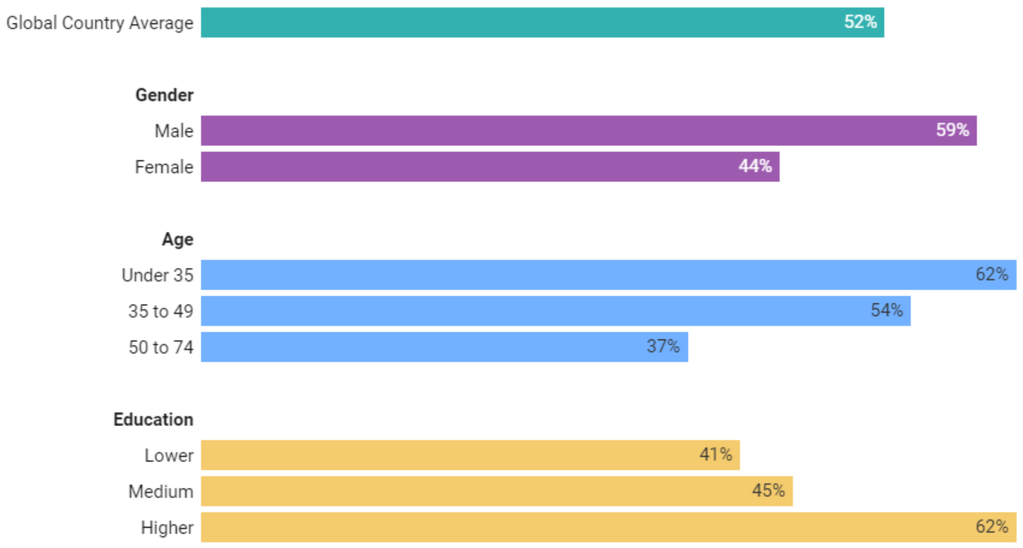
Percentages of those who have done at least one activity in Metaverse.



Note. From “Are immersive experiences creating a new digital divide?,” by the World Economic Forum, 2023b, March 8 (https://www.weforum.org/agenda/2023/01/davos23-immersive-experiences-close-digital-divide/).

Graph 3

Familiarity across demos: How familiar are you with the Metaverse?[4]



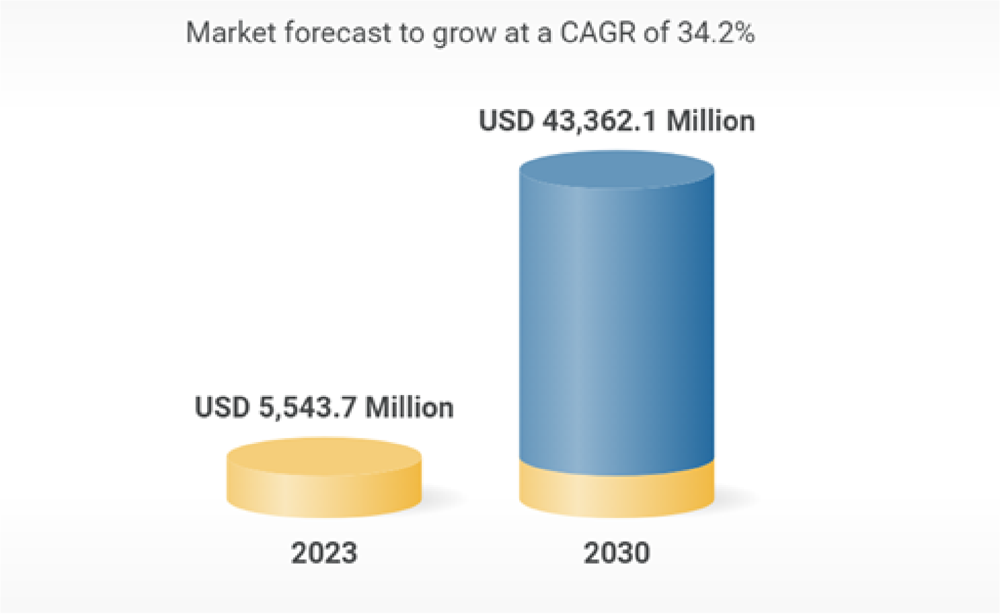
Note. From “How enthusiastic is your country about the rise of the metaverse?,” by the World Economic Forum, March 8

[4] Base: 21,005 online adults under the age of 75 across 29 countries, interviewed April 22-May 6, 2022.

(https://www.weforum.org/agenda/2022/05/countries-attitudes-metaverse-augmented-virtual-reality-davos22/).

Graph 4

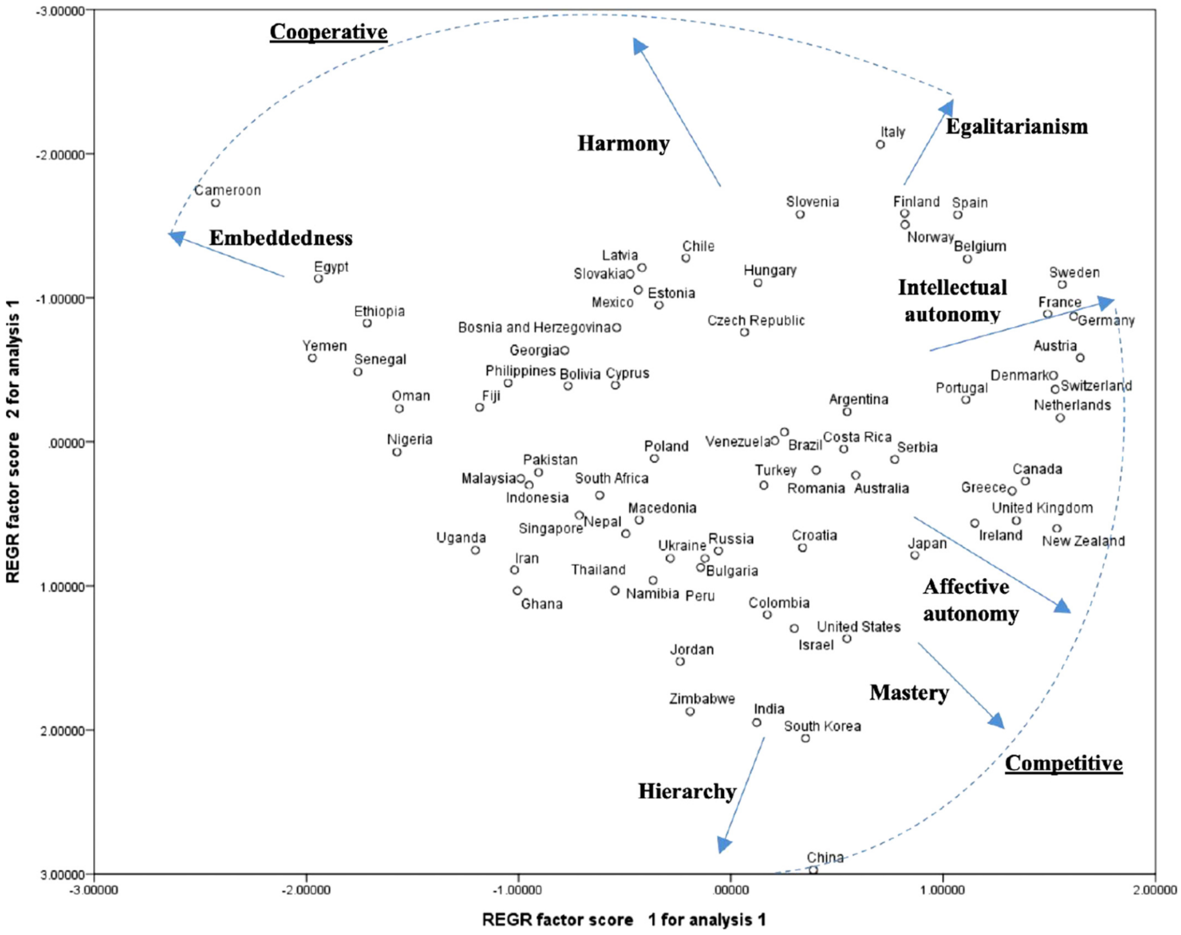
South Korean Metaverse Market



Note. From “South Korea Metaverse Market Intelligence Report 2023: a $43.36 Billion Market by 2030 - Growing Number of South Korean Cities are Seeking a Presence in the Metaverse,” by Research and Markets, *PR Newswire,* May 4, 2023 (https://www.prnewswire.com/news-releases/south-korea-metaverse-market-intelligence-report-2023-a-43-36-billion-market-by-2030---growing-number-of-south-korean-cities-are-seeking-a-presence-in-the-metaverse-301816253.html).

Graph 5

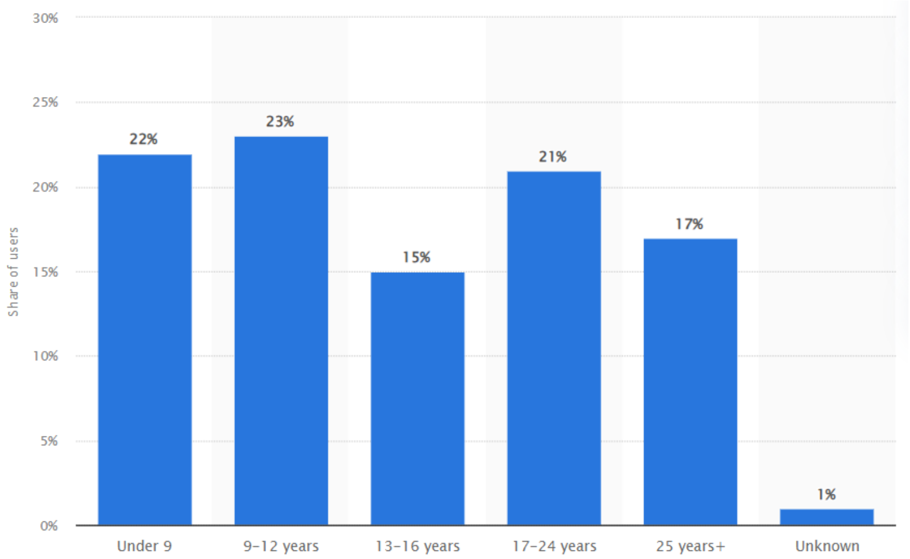
The seven dimensions of the Cooperative versus Competitive cultures



Note. From “Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity,” by Kharlamov, A., & Pogrebna, G. (2021b). *Regulation & Governance,* 15(3), 709–724 (https://doi.org/10.1111/rego.12281).

Graph 6

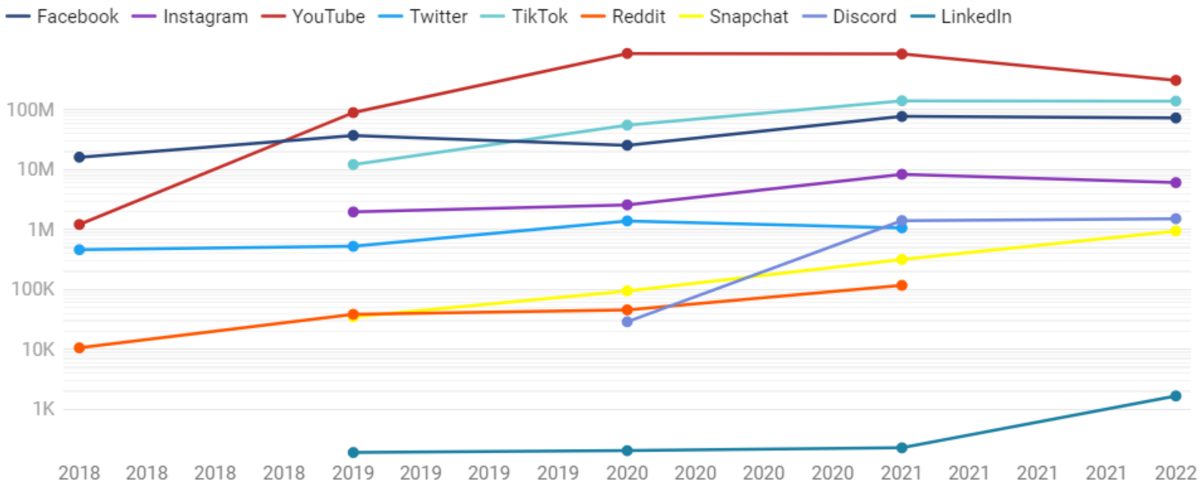
Age distribution of Roblox’s user base, as of December 2022



Note. From “Global Roblox game user distribution by age 2022,” by Statista, April 19, 2023 (https://www.statista.com/statistics/1190869/roblox-games-users-global-distribution-age/).

Graph 7

Social media content and account removals for child abuse and safety - 2018 to Q3 2022[5]

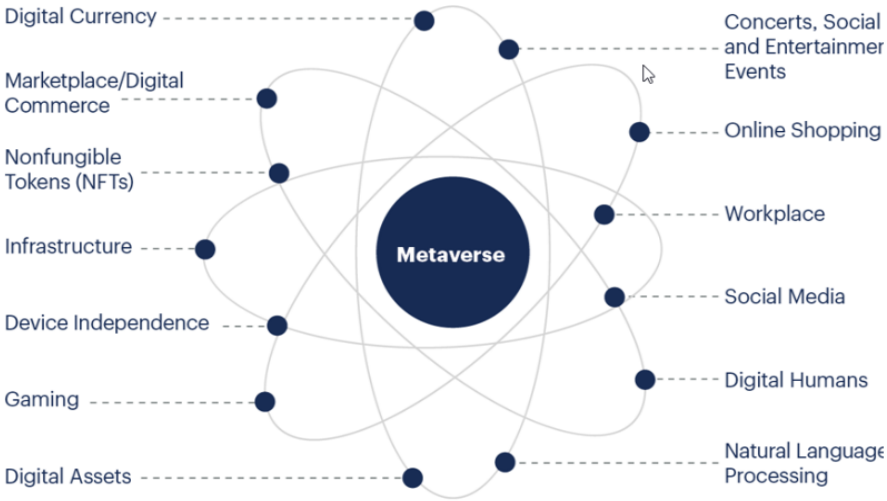


[5] Data unavailable for 2022 for Twitter and Reddit. Facebook, Instagram, YouTube, TikTok, and Discord data for Q1-Q3 of 2021. Snapchat and LinkedIn data for Q1 and Q2 of 2021. YouTube data combined: content, comments, and accounts. Twitter data combined: content and accounts. Discord data combined: content, accounts, and servers.

Note. From “The rising tide of child abuse content on social media,” by Bischoff, P., & Moody, R., *Comparitech,* 2023 (*https://www.comparitech.com/blog/vpn-privacy/child-abuse-online-statistics/*).

Figure 1

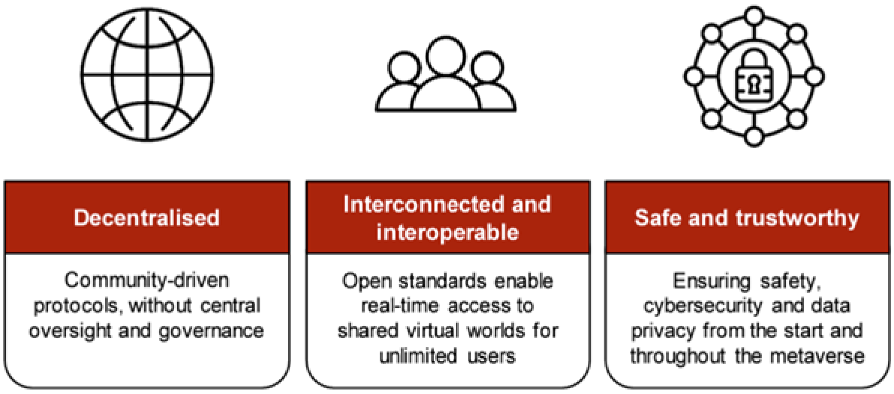
Metaverse Elements



Note. From “What Is a Metaverse? And Should You Be Buying In?,” by Gartner, 2022, as cited in *Metaverse: Opportunities, risks and policy implications | Think Tank | European Parliament*. (n.d.). (https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557).

Figure 2

Key Principles in the Metaverse



Decentralised

Community-driven protocols, without central oversight and governance

Interconnected and interoperable

Open standards enable real-time access to shared virtual worlds for unlimited users

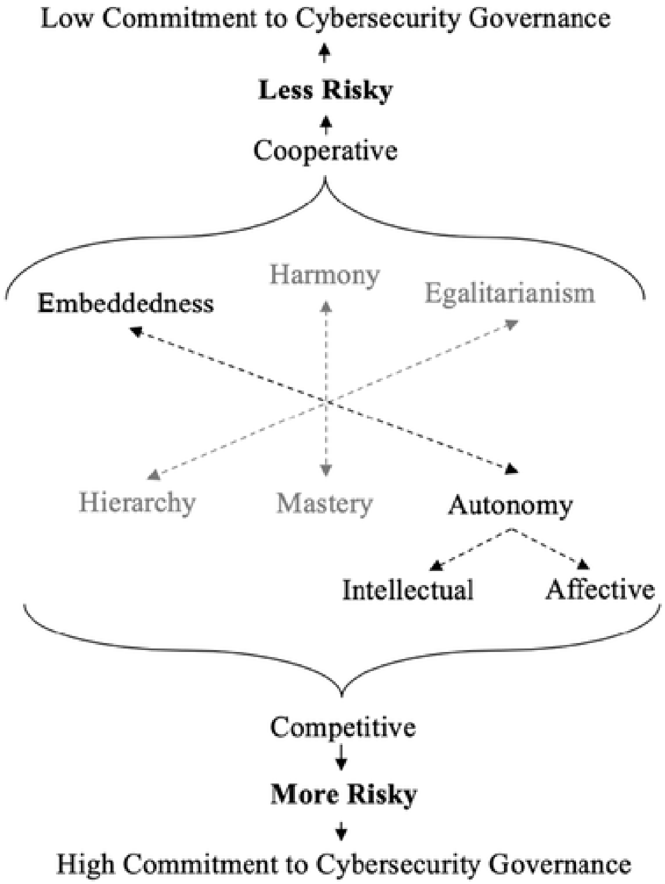
Safe and trustworthy

Ensuring safety, cybersecurity and data privacy from the start and throughout the metaverse

Note. From “The Year Ahead in Digital Policy: Regulating the Metaverse,” by GSMA, *Public Policy*, January 12, 2023 (https://www.gsma.com/publicpolicy/the-year-ahead-in-digital-policy-regulating-the-metaverse).

Figure 3

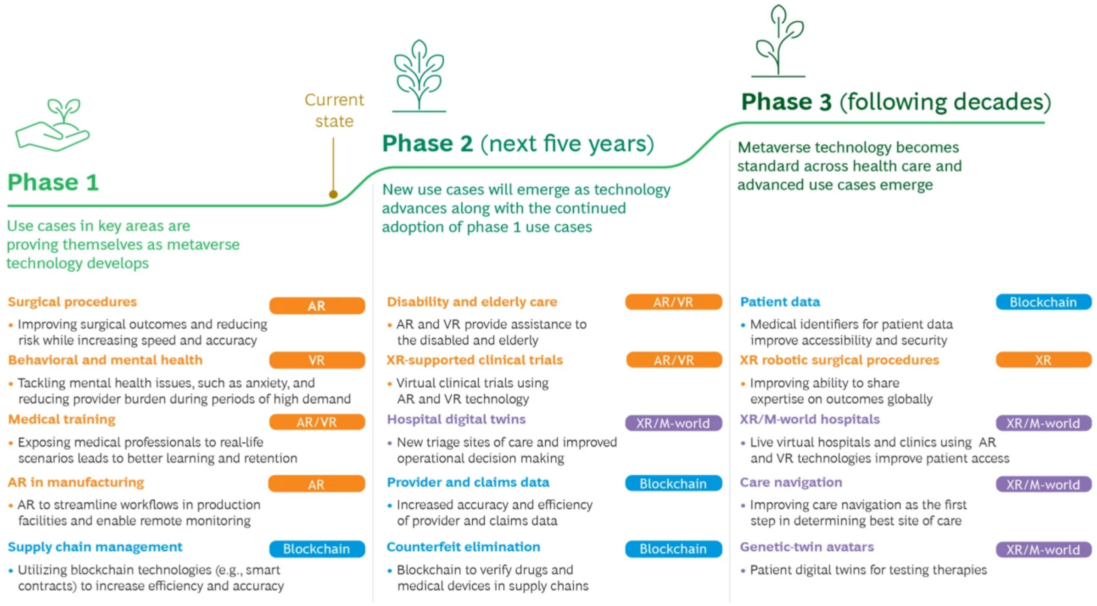
Human values-based framework for cybersecurity regulation



Note. From “Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity,” by Kharlamov, A., & Pogrebna, G. (2021b). *Regulation & Governance,* 15(3), 709–724 (https://doi.org/10.1111/rego.12281).

Table 1

New Use Cases Will Emerge As Metaverse Develops



Current state

Phase 1

Use cases in key areas are proving themselves as metaverse technology develops

Surgical procedures — AR
- Improving surgical outcomes and reducing risk while increasing speed and accuracy

Behavioral and mental health — VR
- Tackling mental health issues, such as anxiety, and reducing provider burden during periods of high demand

Medical training — AR/VR
- Exposing medical professionals to real-life scenarios leads to better learning and retention

AR in manufacturing — AR
- AR to streamline workflows in production facilities and enable remote monitoring

Supply chain management — Blockchain
- Utilizing blockchain technologies (e.g., smart contracts) to increase efficiency and accuracy

Phase 2 (next five years)

New use cases will emerge as technology advances along with the continued adoption of phase 1 use cases

Disability and elderly care — AR/VR
- AR and VR provide assistance to the disabled and elderly

XR-supported clinical trials — AR/VR
- Virtual clinical trials using AR and VR technology

Hospital digital twins — XR/M-world
- New triage sites of care and improved operational decision making

Provider and claims data — Blockchain
- Increased accuracy and efficiency of provider and claims data

Counterfeit elimination — Blockchain
- Blockchain to verify drugs and medical devices in supply chains

Phase 3 (following decades)

Metaverse technology becomes standard across health care and advanced use cases emerge

Patient data — Blockchain
- Medical identifiers for patient data improve accessibility and security

XR robotic surgical procedures — XR
- Improving ability to share expertise on outcomes globally

XR/M-world hospitals — XR/M-world
- Live virtual hospitals and clinics using AR and VR technologies improve patient access

Care navigation — XR/M-world
- Improving care navigation as the first step in determining best site of care

Genetic-twin avatars — XR/M-world
- Patient digital twins for testing therapies

Note. From “The Expanding Health Care Metaverse,” by M., Mérey, T., Adigozel, O., & Busch, N., *BCG Analysis*, 2023 (https://www.bcg.com/publications/2023/the-expanding-reality-of-the-health-care-metaverse).

Table 2

Types of Literature Resources Used in This Study

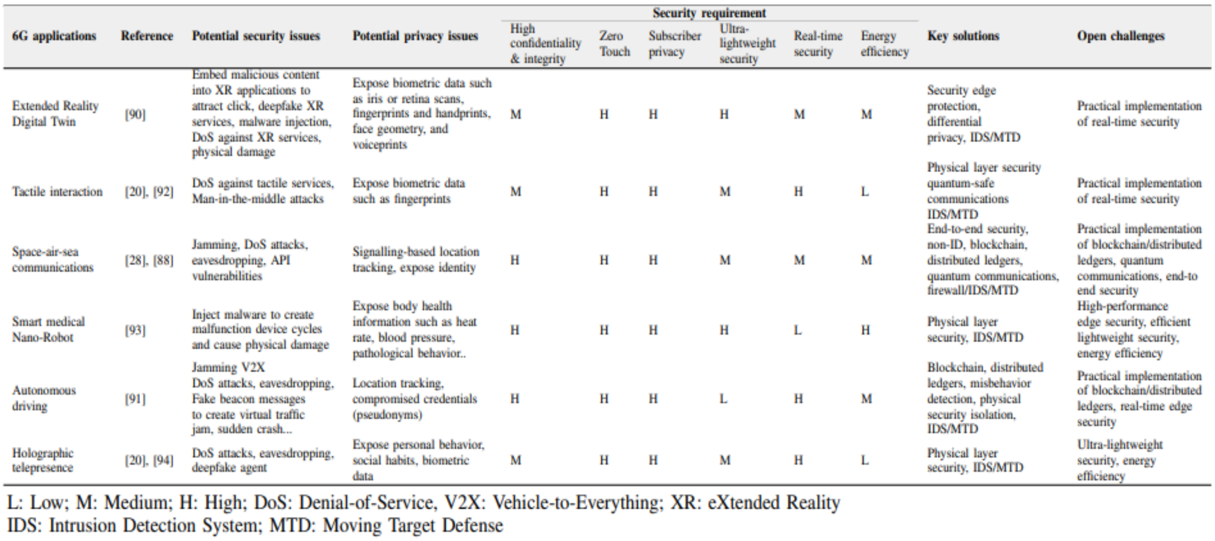
Literature	Examples
Academic papers	Pavlou (2011); Nguyen et al. (2021); Nissenbaum (2009); (Larkina, 2022)
Books	“Privacy in Context: Technology, Policy, and the Integrity of Social Life” by Helen Nissenbaum; “Without a Net: Librarians Bridging the Digital Divide” by Jessamyn West
Reports and statistics	World Economic Forum (WEF) reports
Legal documents and regulations	European General Data Protection Regulation (GDPR)
Industry insights	Epic Games; Meta Platforms; Kaspersky
Government documents and policies	South Korean government Metaverse

	strategy document; ethical roadmap
Press releases	South Korean Ministry of Science and ICT press releases
Online articles	CoinTelegraph; PR Newswire

Note. From “The Overview of Threats and Vulnerabilities in Metaverse” by Issaliyeva (2023).

Table 3

Security and Privacy Issues of Several 6G Applications



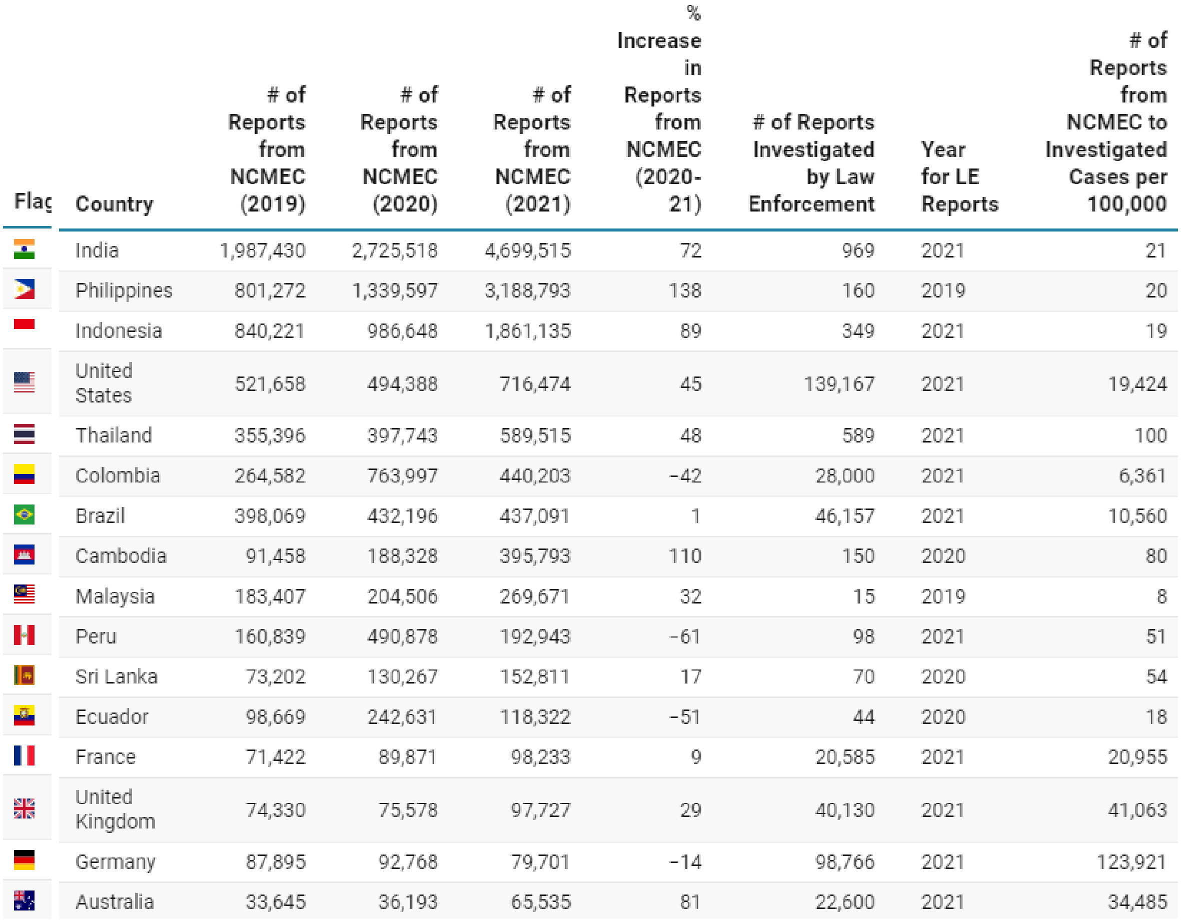
6G applications	Reference	Potential security issues	Potential privacy issues	Security requirement						Key solutions	Open challenges
				High confidentiality & integrity	Zero Touch	Subscriber privacy	Ultra-lightweight security	Real-time security	Energy efficiency		
Extended Reality Digital Twin	[90]	Embed malicious content into XR applications to attract click, deepfake XR services, malware injection, DoS against XR services, physical damage	Expose biometric data such as iris or retina scans, fingerprints and handprints, face geometry, and voiceprints	M	H	H	H	M	M	Security edge protection, differential privacy, IDS/MTD	Practical implementation of real-time security
Tactile interaction	[20], [92]	DoS against tactile services, Man-in-the-middle attacks	Expose biometric data such as fingerprints	M	H	H	M	H	L	Physical layer security quantum-safe communications IDS/MTD	Practical implementation of real-time security
Space-air-sea communications	[28], [88]	Jamming, DoS attacks, eavesdropping, API vulnerabilities	Signalling-based location tracking, expose identity	H	H	H	M	M	M	End-to-end security, non-ID, blockchain, distributed ledgers, quantum communications, firewall/IDS/MTD	Practical implementation of blockchain/distributed ledgers, quantum communications, end-to end security
Smart medical Nano-Robot	[93]	Inject malware to create malfunction device cycles and cause physical damage	Expose body health information such as heat rate, blood pressure, pathological behavior..	H	H	H	H	L	H	Physical layer security, IDS/MTD	High-performance edge security, efficient lightweight security, energy efficiency
Autonomous driving	[91]	Jamming V2X DoS attacks, eavesdropping, Fake beacon messages to create virtual traffic jam, sudden crash...	Location tracking, compromised credentials (pseudonyms)	H	H	H	L	H	M	Blockchain, distributed ledgers, misbehavior detection, physical security isolation, IDS/MTD	Practical implementation of blockchain/distributed ledgers, real-time edge security
Holographic telepresence	[20], [94]	DoS attacks, eavesdropping, deepfake agent	Expose personal behavior, social habits, biometric data	M	H	H	M	H	L	Physical layer security, IDS/MTD	Ultra-lightweight security, energy efficiency

L: Low; M: Medium; H: High; DoS: Denial-of-Service, V2X: Vehicle-to-Everything; XR: eXtended Reality
IDS: Intrusion Detection System; MTD: Moving Target Defense

Note. From “Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges,” by Nguyen, V., Lin, P., Cheng, B., Hwang, R., & Lin, Y. , 2021, *IEEE Communications Surveys and Tutorials*, 23(4), 2384–2428, p.10. (https://doi.org/10.1109/comst.2021.3108618).

Table 4

The number of Reports made from NCMEC to Investigate Online Child Abuse Cases



Flag	Country	# of Reports from NCMEC (2019)	# of Reports from NCMEC (2020)	# of Reports from NCMEC (2021)	% Increase in Reports from NCMEC (2020-21)	# of Reports Investigated by Law Enforcement	Year for LE Reports	# of Reports from NCMEC to Investigated Cases per 100,000
🇮🇳	India	1,987,430	2,725,518	4,699,515	72	969	2021	21
🇵🇭	Philippines	801,272	1,339,597	3,188,793	138	160	2019	20
🇮🇩	Indonesia	840,221	986,648	1,861,135	89	349	2021	19
🇺🇸	United States	521,658	494,388	716,474	45	139,167	2021	19,424
🇹🇭	Thailand	355,396	397,743	589,515	48	589	2021	100
🇨🇴	Colombia	264,582	763,997	440,203	-42	28,000	2021	6,361
🇧🇷	Brazil	398,069	432,196	437,091	1	46,157	2021	10,560
🇰🇭	Cambodia	91,458	188,328	395,793	110	150	2020	80
🇲🇾	Malaysia	183,407	204,506	269,671	32	15	2019	8
🇵🇪	Peru	160,839	490,878	192,943	-61	98	2021	51
🇱🇰	Sri Lanka	73,202	130,267	152,811	17	70	2020	54
🇪🇨	Ecuador	98,669	242,631	118,322	-51	44	2020	18
🇫🇷	France	71,422	89,871	98,233	9	20,585	2021	20,955
🇬🇧	United Kingdom	74,330	75,578	97,727	29	40,130	2021	41,063
🇩🇪	Germany	87,895	92,768	79,701	-14	98,766	2021	123,921
🇦🇺	Australia	33,645	36,193	65,535	81	22,600	2021	34,485

Note. From "The rising tide of child abuse content on social media," by Bischoff, P., & Moody, R., *Comparitech,* 2023 (https://www.comparitech.com/blog/vpn-privacy/child-abuse-online-statistics/).

Glossary

1. **3D Environments**: Digital spaces created or simulated in three dimensions (length, width, and height) to give the effect of a real-life or imaginary scenario.

2. **5G:** The fifth generation of cellular network technology. It enables speeds that can be hundred times faster than 4G. This speed transforms the internet browsing experience, facilitating almost instantaneous downloads and uploads. Additionally, 5G supports a vastly increased device capacity. This means that within a confined area, it can connect thousands of devices simultaneously, without any significant slowdown or loss in performance.

3. **6G:** The sixth generation of mobile technology. While still in development as of 2021, it's expected to bring even higher speeds and lower latency than 5G, alongside other innovations.

4. **Artificial Intelligence (AI)**: The field of science that revolves around the development of computational machines and systems that possess the ability to engage in reasoning, learning, and action and process such volumes of data that are much larger and complex and surpass human analytic capabilities. In essence, this discipline focuses on creating intelligent machines that can replicate, and in some cases exceed, facets of human intelligence, and efficiently process massive amounts of information.

5. **Avatars:** digital personas that represent an individual in a virtual environment and mostly applied in gaming, virtual reality applications, and online communities.

6. **AR (Augmented Reality)**: a technological method that adds different digital elements such as image, sounds, or or other sensory stimuli onto the user's actual physical environment. As an interactive technology, AR can enhance the perception of one's reality.

7. **Blockchain**: decentralised distributed ledger technology, recording transactions across numerous computers. The design ensures that the transactions logged are immutable, meaning they cannot be altered after the fact.

8. **Cyberspace**: vast, interconnected network of digital computing systems and the accompanying digital culture that has grown out of this online integration and connectivity.

9. **Data Breach**: a situation when sensitive, confidential, or protected data is being unlawfully accessed, stolen, or exploited by an anonymous and unauthorised individual. The exposed data may include personal health records, personally identifiable information, corporate trade secrets, or intellectual property.

10. **Digital Twin:** virtual model of a physical entity, system, or process, serving diverse applications, such as simulating scenarios, predicting outcomes, or enhancing performance. Industries like manufacturing, healthcare, and urban planning frequently utilise digital twins.

11. **DoS Attacks (Denial of Service Attacks):** a form of an aggressive cyber-assault on a network where the perpetrator overwhelms the network with an excessive amount of requests. This flood of requests can severely disrupt the normal traffic flow, which then leads to dramatic slow down or complete halt.

12. **DoS Against XR Services:** specific form of DoS attack which can be targeted towards extended reality (XR) services, interrupting their normal functioning.

13. **Edge Computing:** brings data processing and storage closer to the devices(

hence the 'edge' of the network) instead of in a centralised data-processing warehouse. It aims to reduce the bandwidth needed, making data processing more efficient and quicker.

14. **Eavesdropping:** secretly listening to the private conversation or communications of others without their consent, which is often performed with malicious intentions in a digital context.

15. **General Data Protection Regulation (GDPR):** the strongest global legal framework for data protection, which lays out precise rules and protocols for how personal data from individuals living in the European Union should be gathered and processed in order to provide a high level of data privacy and security,

16. **Interoperability:** capacity of different information systems, gadgets, or software applications to exchange, access, and collaboratively use data in a synchronised manner.

17. **IoT (Internet of Things):** interconnected network that encompasses physical devices (ex: everyday household items, appliances, vehicles, sport equipment, etc) which can exchange data with other tech devices or digital systems through the internet.

18. **Malicious Deepfake XR Services:** misuse of extended reality (XR) services using deep fakes, which are synthetic media in which a person's likeness is replaced with someone else's, often with malicious intent.

19. **Malware Injections:** introducing malicious software into a system or network, with the purpose of exploiting system's integrity, confidentiality, or availability of data.

20. **Man-In-The-Middle Attacks:** a cyber attack through which a perpetrator introduces himself into a conversation between two parties; impersonates both parties and eventually gains access to information that they intend to send to each other.

21. **Metaverse:** virtual universe which serves as a shared online space and connects different digital environments, which can eventually allow new immersive experiences for people to live, work, and play in.

22. **Telemedicine:** delivery of healthcare services by using communication technologies or electronic information exchange. This can be used to share critical information for diagnosing, treating, and preventing diseases and injuries or to research and evaluate.

23. **VR (Virtual Reality):** computer-generated simulation of a world, which can either mimic reality or differ from it. This technology can be accessed through

a VR headset.

24. **Web 3.0:** more advanced stage of the internet. It includes machine-processable data and user-created content, which essentially allows web services to become more tailored and context-sensitive.

25. **XR (Extended Reality):** An umbrella term that includes all real-and-virtual combined environments and human-machine interactions generated by computer technology. Ex: AR, MR, VR.

References

A Chinese local court recently opened a hearing in Metaverse, saying it helps drive the digitization of the judicial system - PingWest. (2022). PingWest. https://en.pingwest.com/w/10840

Allsop, J. (2016, October 20). Values in law: how they influence and shape rules and the application of law. Australasian Legal Information Institute. http://classic.austlii.edu.au/au/journals/FedJSchol/2016/15.html

Banco Bilbao Vizcaya Argentaria. (2023, April 19). EU Markets in Cryptoassets (MiCA) Regulation: What is it and why does it matter? NEWS BBVA. https://www.bbva.com/en/innovation/eu-markets-in-cryptoassets-mica-regulation-what-is-it-and-why-does-it-matter/

Bates, D. W., & Samal, L. (2018). Interoperability: What Is It, How Can We Make It Work for Clinicians, and How Should We Measure It in the Future? Health Services Research, 53(5), 3270–3277. https://doi.org/10.1111/1475-6773.12852

Bischoff, P., & Moody, R. (2023). The rising tide of child abuse content on social media. Comparitech. https://www.comparitech.com/blog/vpn-privacy/child-abuse-online-statistics/

Bretton, T. (2022, September 14). People, technologies & infrastructure – Europe's plan to thrive in the metaverse. European Commission - Press Corner. https://ec.europa.eu/commission/presscorner/detail/de/STATEMENT_22_5525

Brewster, T. (2021, October 14). Fraudsters Cloned Company Director's Voice In $35 Million Bank Heist, Police Find. Forbes. https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=36f3f49d7559

Canales, K. (2021, November 20). Mark Zuckerberg's metaverse could fracture the world as we know it — letting people "reality block" things they disagree with and making polarization even worse. Business Insider.

https://www.businessinsider.com/facebook-meta-metaverse-splinter-reality-more-2021-11

Center for Countering Digital Hate (CCDH). (n.d.). Bullying, Sexual Harassment of Minors and Harmful Content are Rife in Meta's Flagship VR Product. Retrieved May 18, 2023, from https://counterhate.com/wp-content/uploads/2023/03/Horizon-Worlds-Exposed_CCDH_0323.pdf?eType=EmailBlastContent&eId=6fb2b25a-6f4c-447b-9ac3-07bd6190feb1

Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021b). The echo chamber effect on social media. Proceedings of the National Academy of Sciences of the United States of America, 118(9). https://doi.org/10.1073/pnas.2023301118

Choi, S. J. (2023, April 12). Regulating the Metaverse in Europe | Global Policy Watch. Global Policy Watch. https://www.globalpolicywatch.com/2023/04/regulating-the-metaverse-in-europe/#page=1

Congress of The United States. (2021, October 8). Big Tech and Children's Privacy Policy Change. Senate.gov. Retrieved May 10, 2023, from https://www.markey.senate.gov/imo/media/doc/ftc_big_tech_childrens_privacy_policy_changes.pdf

Commission welcomes political agreement on the European Chips Act. (2023, April 18). European Commission - Press Corner. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2045

五部门关于印发《虚拟现实与行业应用融合发展行动计划（2022—2026年）》的 通知 (Wǔ bùmén guānyú yìnfā "xūnǐ xiànshí yǔ hángyè yìngyòng rónghé fāzhǎn xíngdòng jìhuà (2022—2026 nián)" de tōngzhī). (n.d.). (Translation: "*Five departments on the issuance of the 'Virtual Reality and Industry Application Integration Development Action Plan* (2022-2026)' Notice"). https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2022/art_775aaa3f77264817a5b41421a8b2ce22.html

Communications Surveys and Tutorials, 23(4), 2384–2428. https://doi.org/10.1109/comst.2021.3108618

Cunningham, C., Ederer, F., & Wang, Y. (2018). Killer Acquisitions. Social Science Research Network. https://doi.org/10.2139/ssrn.3241707

Dean, B. (2023, March 27). Roblox User and Growth Stats 2023. Backlinko. https://backlinko.com/roblox-users

Defining and Building the Metaverse. (n.d.). https://initiatives.weforum.org/defining-and-building-the-metaverse/home

DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R. C., Fox, R., Albright, J., & Johnson, B. (2018). The tactics & tropes of the Internet Research Agency. Retrieved from https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1003&context=senatedocs

Dionisio, J. D. N., Burns, W. C. G., & Gilbert, R. E. (2013). 3D Virtual worlds and the metaverse. ACM Computing Surveys, 45(3), 1–38. https://doi.org/10.1145/2480741.2480751

EMOTIV. (2022, August 2). What is Data Privacy? Definition & FAQs | EMOTIV. https://www.emotiv.com/glossary/data-privacy/

Fallis, D. (2020). The Epistemic Threat of Deepfakes. Philosophy & Technology, 34(4), 623–643. https://doi.org/10.1007/s13347-020-00419-2

Gartner. (n.d.). What Is a Metaverse? And Should You Be Buying In? Gartner. https://www.gartner.com/en/articles/what-is-a-metaverse

Gaur, N. (2022, January 1). DAOs are the foundation of Web3, the creator economy and the future of work. Cointelegraph. https://cointelegraph.com/news/daos-are-the-foundation-of-web3-the-creator-economy-and-the-future-of-work

Global Risks Report 2023 | World Economic Forum. (n.d.). World Economic Forum. https://www.weforum.org/reports/global-risks-report-2023/

GSMA. (2023, January 12). The Year Ahead in Digital Policy: Regulating the Metaverse | Public Policy. Public Policy. https://www.gsma.com/publicpolicy/the-year-ahead-in-digital-policy-regulating-the-metaverse

Han, Y., Zhang, Y., & Vermund, S. H. (2022b). Blockchain Technology for Electronic

Health Records. International Journal of Environmental Research and Public Health, 19(23), 15577. https://doi.org/10.3390/ijerph192315577

Hern, A. (2022b, October 28). Meta shares dip is proof metaverse plan never really had legs. The Guardian. https://www.theguardian.com/technology/2022/oct/27/metas-shares-dip-is-proof-metaverse-plan-never-really-had-legs-facebook

Hui, M. (2022, November 3). China is bringing industrial policy to the metaverse. Quartz. https://qz.com/china-is-bringing-industrial-policy-to-the-metaverse-1849736425

Identity Defined Security Alliance. (2023, January 31). 2022 Trends in Securing

Digital Identities | Identity Defined Security Alliance. https://www.idsalliance.org/white-paper/2022-trends-in-securing-digital-identities/

Identity Theft and Assumption Deterrence Act. (2013, August 12). Federal Trade Commission. https://www.ftc.gov/node/119459

Info. (2023, March 8). Metaverse Insights in South Korea. AJ Marketing. https://www.ajmarketing.io/post/metaverse-insights-in-south-korea

Irshad, S., & Soomro, T. R. (2018). Identity Theft and Social Media. ResearchGate. https://www.researchgate.net/publication/323185128_Identity_Theft_and_Social_Media

Koops, B., & Leenes, R. (2006). Identity theft, identity fraud and/or identity-related crime. Datenschutz Und Datensicherheit - Dud, 30(9), 553–556. https://doi.org/10.1007/s11623-006-0141-2

Kharpal, A. (2021, August 30). TikTok owner ByteDance takes first step into virtual reality with latest acquisition. CNBC. https://www.cnbc.com/2021/08/30/tiktok-owner-bytedance-acquires-pico-and-takes-first-step-into-virtual-reality.html

Kharpal, A. (2022, March 29). Alibaba leads $60 million funding into augmented reality glasses maker Nreal in metaverse play. CNBC. https://www.cnbc.com/2022/03/29/alibaba-nreal-60-million-funding-round-metaverse-play.html

Klosowski, T. (2021, September 8). The State of Consumer Data Privacy Laws in the US (And Why It Matters). Wirecutter: Reviews for the Real World. https://www.nytimes.com/wirecutter

Kharlamov, A., & Pogrebna, G. (2021). Using human values‐based approach to understand cross‐cultural commitment toward regulation and governance of cybersecurity †. Regulation & Governance, 15(3), 709–724. https://doi.org/10.1111/rego.12281

Larkina, A. (2022, November 25). Consumer cyberthreats: predictions for 2023. Securelist. https://securelist.com/consumer-threats-2023/108112/

Li, J., Chaudhuri, S., & Rafiq, A. (2021). Metaverse Economy: Digital Life Beyond the Screen. DBS Bank. https://www.dbs.com/insights/metaverse-economy-digital-life-beyond-the-screen

Liu, W. (2022, December 23). Chinese internet companies launch a wave of new businesses to explore the metaverse. 36Kr. https://36kr.com/p/1462811577326723

Linden Lab. (n.d.). https://www.lindenlab.com/releases/high-fidelity-invests-in-second-life#:~:text=ABOUT%20SECOND%20LIFE&text=First%20launched%20in%202003%2C%20Second,%24650%20million%20(USD)%20economy.%20%20https://academy.binance.com/en/articles/what-is-blockchain-technology-a-comprehensive-guide-for-beginners

Lindgren, R., Tscholl, M., Wang, S., & Johnson, E. (2016). Enhancing learning and engagement through embodied interaction within a mixed reality simulation. Computers & Education, 95, 174–187. https://doi.org/10.1016/j.compedu.2016.01.001

Ltd, R. a. M. (n.d.). South Korea Metaverse Market Intelligence and Future Growth Dynamics Databook - 100+ KPIs Covering Market Size by Sector X Use cases X Technology, Business and Consumer Spend, NFT Spend - Q1 2023. Research and Markets Ltd 2023. https://www.researchandmarkets.com/reports/5738842/south-korea-metaverse-market-intelligence-future?utm_source=CI&utm_medium=PressRelease&utm_code=33s9xr

Maloney, Divine, "A Youthful Metaverse: Towards Designing Safe, Equitable, and Emotionally Fulfilling Social Virtual Reality Spaces for Younger Users" (2021). All Dissertations. 2931. https://tigerprints.clemson.edu/all_dissertations/2931

Mann, J. (2022, October 29). Mark Zuckerberg says Facebook is becoming Meta in major rebrand. CNN. https://edition.cnn.com/2022/10/28/tech/facebook-change-name-meta/index.html

Market, V. O. T. (2022, April 8). H1 2021 digital health funding: Another blockbuster year. . .in six months | Rock Health. Rock Health | We're Powering the Future of Healthcare. Rock Health Is a Seed and Early-stage Venture Fund That Supports Startups Building the Next Generation of Technologies Transforming Healthcare. https://rockhealth.com/insights/h1-2021-digital-health-funding-another-blockbuster-year-in-six-months/

Martin, K. E. (2016). Understanding Privacy Online: Development of a Social Contract Approach to Privacy. Journal of Business Ethics, 137(3), 551–569. https://doi.org/10.1007/s10551-015-2565-9

Mathews, M., Mérey, T., Adigozel, O., & Busch, N. (2023). The Expanding Health Care Metaverse. BCG Global. https://www.bcg.com/publications/2023/the-expanding-reality-of-the-health-care-metaverse

Mello-Klein, C. (2022). Why is Mark Zuckerberg's Metaverse failing? Northeastern Global News. https://news.northeastern.edu/2022/11/03/metaverse-failure/

The Metaverse - GlobalData. (2023). GlobalData. https://www.globaldata.com/metaverse/

McKinsey & Company. (2021, July 9). Telehealth: A quarter-trillion-dollar post-COVID-19 reality? McKinsey & Company. https://www.mckinsey.com/industries/healthcare/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality

McQue, K., & McNamara, M. (2023, May 22). How Facebook and Instagram became marketplaces for child sex trafficking. The Guardian. https://www.theguardian.com/news/2023/apr/27/how-facebook-and-instagram-became-marketplaces-for-child-sex-trafficking#:~:text=From%20January%20to%20September%202022,and%20Instagram%20reported%206.1m.

Meta share price falls after renaming and metaverse plans (2022, October 29). BBC News. https://www.bbc.com/news/business-59090508

Metaverse Market Size, Share, Industry Trends Analysis By 2028. (n.d.). BrandEssence® Market Research. https://brandessenceresearch.com/technology-and-media/metaverse-market-size

MIT Technology Review. (2022, September 9). Identity protection is key to metaverse innovation. MIT Technology Review. https://www.technologyreview.com/2022/09/12/1058086/identity-protection-is-key-to-metaverse-innovation/

Moore, C. (2022, November 2). How China is building the metaverse. Protocol. https://www.protocol.com/china-report/metaverse-china

Mu, C. (2023, January 20). Chinese Tech Giants Race to Shape National Metaverse Standards. PingWest. https://en.pingwest.com/w/11066

Muhammad, I. (2022). South Korea Shares Blueprint of Its Metaverse Ecosystem. BeyondGames.biz. https://www.beyondgames.biz/19858/south-korea-shares-blueprint-of-its-metaverse-ecosystem/

Nguyen, V., Lin, P., Cheng, B., Hwang, R., & Lin, Y. (2021). Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges. IEEE

Nietzel, M. T. (2023, May 4). NSF Announces $140 Million Investment In Seven Artificial Intelligence Research Institutes. Forbes. https://www.forbes.com/sites/michaeltnietzel/2023/05/04/nsf-announces-140-million-investment-in-seven-artificial-intelligence-research-institutes/?sh=7b79baf34d21

Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79(1), 119–157. https://www.ida.liu.se/~TDDD82/slides/mts/nissenbaum.pdf

Nissenbaum, H. (2009). Privacy in Context.

Nix, N. (2023, March 8). Meta doesn't want to police the metaverse. Kids are paying the price. Washington Post. https://www.washingtonpost.com/technology/2023/03/08/metaverse-horizon-worlds-kids-harassment/

O'Brien, P. (2012, June 12). Should you let your child play in Habbo Hotel? Channel 4 News. https://www.channel4.com/news/should-you-let-your-child-play-in-habbo-hotel

Olson Jr, M. (1971). The Logic of Collective Action: Public Goods and the Theory of Groups, with a new preface and appendix (Vol. 124). Harvard University Press.

Ong, T. (2022, November 15). Metaverse platforms can be addictive and harmful, Tencent warns. The Verge. https://www.theverge.com/2022/11/15/22784713/tencent-metaverse-addictive-harmful

Pannone, A. (2023). China as a technology leader for the Metaverse in 2023, report by Globaldata. *The Cryptonomist*. https://en.cryptonomist.ch/2023/03/20/china-leader-metaverse-2023/

Pavlou, P. A. (2011). State of the Information Privacy Literature: Where are We Now And Where Should We Go? Management Information Systems Quarterly, 35(4), 977. https://doi.org/10.2307/41409969

Pessarlay, W. (2022). South Korea's Science Ministry unveils metaverse strategy, ethical principles for industry operators. CoinGeek. https://coingeek.com/south-korea-science-ministry-unveils-metaverse-strategy-ethical-principles-for-industry-operators/

Pessarlay, W. (2022, January 1). DAOs are the foundation of Web3, the creator economy and the future of work. Cointelegraph. https://cointelegraph.com/news/daos-are-the-foundation-of-web3-the-creator-economy-and-the-future-of-work

Pessarlay, W. (2022a). Japan establishes 'Web 3.0 Policy Office' to formulate metaverse-related policies. CoinGeek. https://coingeek.com/japan-establishes-web-3-0-policy-office-to-formulate-metaverse-related-policies/

Pham, S. (2023, March 31). The metaverse is a trillion-dollar opportunity for Microsoft, Citi says. CNBC. https://www.cnbc.com/2023/03/31/citi-the-metaverse-is-a-trillion-dollar-opportunity-for-microsoft.html

Phippen, A. (2022, March 23). Protecting children in the metaverse: it's easy to blame big tech, but we all have a role to play. Parenting for a Digital Future. https://blogs.lse.ac.uk/parenting4digitalfuture/2022/03/23/metaverse/

PingWest. (2022b). Baidu officially enters the metaverse, launching its own VR platform. PingWest. https://en.pingwest.com/a/14597

Press Releases - 과학기술정보통신부 >. (n.d.-c). https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=650

Reed, K. (2022, November 29). Metaverse Regulatory Uncertainty: What it Means for Investors. Finance Magnates. https://www.financemagnates.com/metaverse-regulatory-uncertainty-what-it-means-for-investors/

Ringma, M. (2023). Digital doppelgängers and evil twins: How brands can guard against identity theft and fraud in the metaverse. Fast Company. https://www.fastcompany.com/90841499/digital-doppelgangers-and-evil-twins-how-brands-can-guard-against-identity-theft-and-fraud-in-the-metaverse

Robitzski, D. (2022, July 21). One Company May Have Finally Cracked Brain-Machine Interfaces. Freethink. https://www.freethink.com/articles/brain-machine-interface

Rock Health. (2022, April 8). H1 2021 digital health funding: Another blockbuster year. . .in six months | Rock Health. Rock Health | We're Powering the Future of Healthcare. Rock Health Is a Seed and Early-stage Venture Fund That Supports Startups Building the Next Generation of Technologies Transforming Healthcare. https://rockhealth.com/insights/h1-2021-digital-health-funding-another-blockbuster-year-in-six-months/

Ruby, D. (2023). 105+ Metaverse Statistics For 2023 (Users & Market Trends). Demand Sage. https://www.demandsage.com/metaverse-statistics/#:~:text=Metaverse%20has%20400%20million%20monthly%20active%20users%20as%20of%202023

Ruby, D. (2023b). Roblox Statistics 2023 — (Demographics & Financials). Demand Sage. https://www.demandsage.com/how-many-people-play-roblox/#:~:text=Currently%2C%20Roblox%20currently%20has%2066.1,we%20are%20covering%20it%20all!

Sandeepa, C., Wang, S., & Liyanage, M. (2023). Privacy of the Metaverse: Current Issues, AI Attacks, and Possible Solutions. ResearchGate. https://www.researchgate.net/publication/369331696_Privacy_of_the_Metaverse_Current_Issues_AI_Attacks_and_Possible_Solutions

Shi, S., He, D., Li, L., Kumar, N., Khan, M. S., & Choo, K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & Security, 97, 101966. https://doi.org/10.1016/j.cose.2020.101966

Slade, M. (2022, January 10). The Future of Work in the Metaverse. Salesforce.com. https://www.salesforce.com/blog/future-of-work-in-the-metaverse/

Smith, B. a. C. a. T. (2022, February 23). Metaverse app allows kids into virtual strip clubs. BBC News. https://www.bbc.com/news/technology-60415317

Smith, E. (2023, April 20). Facebook’s metaverse transition is a ‘hail Mary’ to find new ad growth, say former employees. CNBC. https://www.cnbc.com/2023/04/20/facebooks-metaverse-transition-is-a-hail-mary-to-find-new-ad-growth-say-former-employees.html

Statista. (2022, June 28). *Consumers witnessing false information on certain topics worldwide 2022, by region*. https://www.statista.com/statistics/1317019/false-information-topics-worldwide/

Statista. (n.d.-b). *Metaverse - United States | Statista Market Forecast*. https://www.statista.com/outlook/amo/metaverse/united-states

Stephenson, N. (1994). Snow Crash. Penguin UK.

Sun, T. R., He, X., Song, X., Shu, L., & Li, Z. (2022). The Digital Twin in Medicine: A Key to the Future of Healthcare? Frontiers in Medicine, 9, 907066. https://doi.org/10.3389/fmed.2022.907066

Takemoto, Y., & Lee, J. (2023, April 22). Japan proposes guidelines for metaverse development. Nikkei Asia. https://asia.nikkei.com/Business/Technology/Japan-proposes-guidelines-for-metaverse-development

Telehealth: A quarter-trillion-dollar post-COVID-19 reality? (2021, July 9). McKinsey & Company. https://www.mckinsey.com/industries/healthcare/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality

TechCrunch is part of the Yahoo family of brands. (2023, February 3). https://techcrunch.com/2023/02/03/metas-reality-labs-lost-13-7-billion-on-vr-and-ar-last-year/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAK3NKlwM-gLJCLs2th5XhLeXsjTReEdXrq3DyJ9uex8k2nuXynAWeoxVgdC4VQ9YZZbRe34ex_1bnpt5-OfQdAZRDwFmNQHqBTSrSMOW8ewGIyI3xEfoQ9ctLgys_-b-E0I-kEcFVNl4nA6zjh-AARXA_2LJYgMJpYJhxfpvqtrc

Translation: 14th Five-Year Plan for National Informatization – Dec. 2021 - DigiChina. (2022, January 24). DigiChina. https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/

The Future of Cybersecurity and Privacy. (2021, July). Deloitte Insights. https://www2.deloitte.com/us/en/insights/industry/financial-services/future-of-cybersecurity-and-privacy.html

This chart shows how big the metaverse market could become. (2023, March 8). World Economic Forum. https://www.weforum.org/agenda/2023/02/chart-metaverse-market-growth-digital-economy/

中国电子信息产业发展研究院. (2022). 2023年中国虚拟现实产业发展预测报告. 中国电子信息产业发展研究院. (Translation: "2023 China Virtual Reality Industry Development Forecast Report" by China Electronics Information Industry Development Research Institute). https://www.ccidconsulting.com/research/hybg/56258.html

杨希 (Yang Xi). (2021). Chinese firms and investors race into the metaverse as experts call for rational development - China.org.cn. http://www.china.org.cn/business/2021-12/01/content_77904687.htm

Vaccari, C., & Chadwick, A. (2020). Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. Social Media and Society, 6(1), 205630512090340. https://doi.org/10.1177/2056305120903408

Waltzman, R. (2022, August 22). Facebook misinformation is bad enough. The metaverse will be worse. Washington Post. https://www.washingtonpost.com/opinions/2022/08/22/metaverse-political-misinformation-virtual-reality/

Wasike, B. (2022). Memes, Memes, Everywhere, nor Any Meme to Trust: Examining the Credibility and Persuasiveness of COVID-19-Related Memes. Journal of Computer-Mediated Communication, 27(2). https://doi.org/10.1093/jcmc/zmab024

Web 3.0 Policy Office Established in the Minister's Secretariat as a Cross-Departmental Internal Organization. (2022, July 15). Ministry of Economy, Trade and Industry (METI). https://www.meti.go.jp/english/press/2022/0715_002.html

Weissberger, A. (2022, November 23). SK Telecom launches its metaverse platform 'ifland' in 49 countries and regions – Technology Blog. https://techblog.comsoc.org/2022/11/23/sk-telecom-launches-its-metaverse-platform-ifland-in-49-countries-and-regions/

Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review, 9(11), 39–52. https://doi.org/10.22215/timreview/1282

What Is a Metaverse? And Should You Be Buying In? (n.d.). Gartner. https://www.gartner.com/en/articles/what-is-a-metaverse

What Is Minecraft Education? (n.d.). education.minecraft.net. https://education.minecraft.net/en-us/discover/what-is-minecraft

What is a digital twin? | IBM. (n.d.). https://www.ibm.com/topics/what-is-a-digital-twin#:~:text=A%20digital%20twin%20is%20a,reasoning%20to%20help%20decision-making

Winkelman, R. (2022, February 28). Microsoft Mesh could shape the metaverse. VentureBeat. https://venturebeat.com/2022/02/28/microsoft-mesh-could-shape-the-metaverse/

With Increasing Usage of Virtual Reality Platforms and Devices, Senator Markey and Reps. Castor, Trahan Urge FTC to Monitor Threats to Children in the Metaverse | U.S. Senator Ed Markey of Massachusetts. (2022, February 16). Edward Markey. https://www.markey.senate.gov/news/press-releases/with-increasing-usage-of-virtual-reality-platforms-and-devices-senator-markey-and-reps-castor-trahan-urge-ftc-to-monitor-threats-to-children-in-the-metaverse

Wong, S.-L., Shepherd, C., & Liu, Q. (2019, September 3). Old messages, new memes: Beijing's propaganda playbook on the Hong Kong protests. Financial Times. https://www.ft.com/content/7ed90e60-ce89-11e9-99a4-b5ded7a7fe3f

World Economic Forum. (2023, March 8). This chart shows how big the metaverse market could become. https://www.weforum.org/agenda/2023/02/chart-metaverse-market-growth-digital-economy/

Wu, L., Morstatter, F., Carley, K. M., & Liu, H. (2019b). Misinformation in Social Media. SIGKDD Explorations, 21(2), 80–90. https://doi.org/10.1145/3373464.3373475

Zacks. (2023, April 20). Are Metaverse ETFs the Next Big Thing? Zacks.com. https://www.zacks.com/stock/news/1856105/are-metaverse-etfs-the-next-big-thing

Zarei, K., Farahbakhsh, R., Crespi, N., & Tyson, G. (2020). Impersonation on Social Media: A Deep Neural Approach to Identify Ingenuine Content. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2010.08438