International Journal of Religion
2024
Volume: 5| Number 12 | pp. 684 – 698
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/gy897963

Influence of Technology and Metaverse on Traditional Absolute Sovereignty Control of Modern National States Territories

Mahmoud Kaleem[1]

Abstract

The metaverse can extend the physical world using augmented and virtual reality technologies, allowing users to seamlessly interact within virtual and simulated environments using avatars and holograms. This investigation strives to analyze the relationship between technology and the metaverse on traditional absolute sovereignty control of modern national states' territories to understand better the potential impact of emerging virtual environments on the established structures and systems of physical governance. As technology continues to evolve and the metaverse grows in size and complexity, examining how it may challenge traditional notions of territorial sovereignty and governance is essential. It can occur in several ways, such as borderless access, jurisdictional disputes, decentralization of power, and cyber security concerns. Based on secondary data, the study showed different ways technology and the metaverse intersect with traditional state control. It can identify potential conflict areas and develop strategies to adapt to this rapidly evolving landscape. Therefore, it is to gain a deeper understanding of the complex relationship between technology, the metaverse, and the traditional structures of governance that have shaped our world. The ultimate goal is to structure the metaverse in morally acceptable ways and collectively the most democratically beneficial for society.

Keywords: *Metaverse, Technology, Sovereignty Control, States Territories*

INTRODUCTION

Although the metaverse is a relatively recent addition to the everyday lexicon of technology commentators and academics alike, the term was first used in 1992 in a Neal Stephenson novel. The term "metaverse" refers to a shared virtual reality environment, often depicted in science fiction, where users can interact with each other and digital objects in a simulated world (Dwivedi et al., 2022). The idea of a metaverse has been around for decades. However, technological advances have made it increasingly feasible to create and experience virtual reality environments in new and more immersive ways. Metaverses are accessible through virtual reality (VR) headsets, glasses, or other dedicated devices. It facilitates the purchase or rental of virtual real estate (Tucci, 2022), provides services and experiences to users (Weston, 2022), and utilizes virtual avatars for social connection (Downs, 2022). Mark Zuckerberg, CEO of Facebook, has described the metaverse as the "holy grail of social interactions" (Newton, 2021). It will be an online "phygital world" where physical and virtual realities merge (Buckler, 2022).

Technology development has had a significant impact on the metaverse, enabling the creation of more complex and realistic virtual reality environments and online games (Joshua, 2017). It includes advancements in computer graphics, virtual reality, artificial intelligence, and blockchain technology (Lee et al., 2021a; The Verge, 2021). These technologies have enabled the creation of virtual worlds with rich and detailed environments where users can engage in gaming, socializing, and commerce. Organizations are starting to assess the potential of the metaverse and how it can be integrated into their existing business models.

The metaverse is poised to become an increasingly important part of our lives (Purdy, 2022) as more and more people turn to virtual reality environments as a means of escape, entertainment, and connection. At the same time, however, the rise of the metaverse raises important questions about privacy, security, regulation, and the future of state sovereignty in the digital age (Artz, 2022). States of all sizes have explored the concept of the metaverse. The metaverse poses opportunities for state actors to capitalize on its potential. However, it also

[1] Associate Professor, College of Media, Department of Pubic Relation and Advertising City University Ajman, United Arab Emirates E-mail: m.kaleem@cuca.ae

raises questions about military capabilities, social injustices, property rights, economic aid and development, and cultural exchanges (Greenwald, 2022).

Internet governance and domestic law operation vary considerably from country to country, and the metaverse will exacerbate rather than flatten this trend. A single metaverse will not provide a common global experience due to each country or region's unique set of favorable laws and social norms (Garon, 2022). Barbados' recent launch of a virtual embassy is an example of how states are beginning to make their presence known in the metaverse (Wyss, 2021). This move is significant as it shows that traditional absolute sovereignty control of modern national state territories can be extended into the digital realm (Casey, 2021). In traditional nations, citizens are defined by the Nation-State that assigns identities to unique physical persons. Citizenship has certain rights and responsibilities, which can now be extended into virtual worlds through digital nations (Over, 2022).

The Impact of Technology on Traditional Sovereignty

The impact of technology on traditional sovereignty has been substantial in recent years. Technology has challenged the traditional concept of sovereignty by changing how states and individuals interact (Bellanova et al., 2021). The increasing interconnectedness of technology has led to a reconfiguration of power relationships between states and individuals. It has had far-reaching consequences for the nature and exercise of sovereignty. One of the primary ways technologies have impacted traditional sovereignty is through the growth of global communication networks. The internet and social media have enabled people to connect quickly and communicate across borders (Riddle, 2017), giving individuals and groups new avenues for expressing their opinions and mobilizing collective action. It has led to a democratization of information and empowering individuals in previously impossible ways.

Another way in which technology has impacted traditional sovereignty is through the increasing interconnectedness of the global economy. Advances in transportation and communication technologies have made it easier for businesses to operate across borders, leading to the growth of multinational corporations (Ahi et al., 2022) and the increasing interdependence of countries. It has made it more difficult for states to regulate their economies and control the flow of goods and capital across their borders. A third-way technology has impacted traditional sovereignty is through the growing importance of cyber security. The deepening dependency on the internet and technology has created new vulnerabilities for states and individuals, leading to a growing concern about the security of critical infrastructure and personal data. States are grappling with how to respond to these new threats and protect their citizens, which has challenged traditional notions of sovereignty and state control.

Finally, technology has also impacted traditional sovereignty by growing new actors and stakeholders (Edler et al., 2021). For example, companies like Google and Facebook have become significant players in shaping global discourse and decision-making (Lauer, 2021). The companies have profoundly impacted our access to ideas, information, and one another. It has an unprecedented global reach and, in many markets, serves as a de-facto monopolist. Its influence over individual and global affairs is unique in human history. It has created new challenges for states as they try to balance the interests of these new actors with those of their citizens.

The Rise of Virtual States and Jurisdictions in the Metaverse

The rise of virtual states and jurisdictions in the metaverse refers to the emergence of virtual territories and communities within virtual reality environments and online games (Ball, 2020; Balkin, 2017). The metaverse is a virtual realm where many real-world actions are emulated (Mileva, 2023). It is accessed through games that leverage crypt currencies or non-fungible tokens (NFTs). The growing popularity of extended reality (XR) is one factor that will continue to shape the metaverse. The metaverse is an all-encompassing digital world that is parallel to the real world. It can offer companies opportunities to find solutions online and apply them to the real world (Shone & Humairah, 2022).

State powers are beginning to make their presence known in the metaverse, as Barbados launches a virtual embassy and China leverages its dedicated blockchain research group to harness data in virtual worlds (Greenwald, 2022). The innovation of the metaverse and its capacity can support different methods. There is an opportunity for states to differentiate themselves virtually, developing a broader range of potentials and concerns such as military capabilities, social injustices, property rights, economic aid and development, and cultural exchanges (Greenwald, 2022).

The form of jurisdiction most relevant to the metaverse may be universal jurisdiction, which recognizes state jurisdiction over certain crimes regardless of where or by whom they were committed (Cooper, 2021). As Meta (formerly Facebook) and other technology companies prepare for their versions of the coming "metaverse," it would be wise to figure out the rules to be applied inside these virtual worlds ahead of time. Terms of service from Big Tech do not often protect fundamental human rights. Suppose the metaverse is to unleash the full potential of the internet. In that case, it should not be stymied by nefarious actors, Big Tech, or self-interested states exercising their power over it (Cooper, 2021).

The emergence of virtual states and jurisdictions in the metaverse has created new challenges for traditional governance structures. For example, disputes between users within virtual environments can be challenging to resolve, and virtual communities may have different norms and values that conflict with those of the real world. As the metaverse continues to grow, we will likely see the development of new governance structures and legal systems to address these challenges and ensure the stability and security of these virtual communities.

The Regulation of Digital Assets and Virtual Economies

The regulation of digital assets and virtual economies refers to the laws and policies that govern the creation, transfer, and use of digital assets within virtual reality environments and online games. Digital assets are digital representations of value that can be traded and used for various purposes, such as virtual currency, virtual goods, and virtual real estate. Virtual economies exist within these virtual environments, where users can earn, trade, and spend digital assets.

For instance, the United States government has issued an executive order to ensure the responsible development of digital assets to protect consumers, investors, and businesses (The White House, 2022). The United States Securities and Exchange Commission (SEC) can play a role in regulating digital assets that are securities. Digital assets have largely been unregulated, which has led to frequent price manipulation, fraud, exploitation, theft of assets, and unpaid taxes (Phillips, 2021). Governments recognize the risks of a fast-growing sector that has developed mainly outside the perimeters of financial regulation or even credible understanding (Desir, 2022).

Desir (2022) explained that regulators tasked with overseeing a sustainable crypto ecosystem would seek to build legal and supervisory frameworks that will enable them to detect and prevent financial crime, establish good corporate governance standards, and require beneficial ownership disclosures. The Basel Committee on Banking Supervision has proposed global rules for digital assets with differing risk weightings. The researcher also posited that tokenized traditional assets and stable coins backed by fiat currencies would be treated like loans.

The Office of the Comptroller of Currency (OCC) provides policy, guidance, advisories, and information about the use of digital assets in the federal banking system (OCC, 2023). Controllers at both the national and state levels have been working on trying to protect consumers and investors, safeguard the financial system, and allow for innovation and competition. The Center on Regulation and Markets convened an event regulating digital assets where regulators discussed how Congress should respond to digital assets. They stressed the need for Congress to appropriate significant funding for the regulation of the market (Brookings, 2022).

Digital assets can take many different forms and have a range of functions, making it difficult to determine how they should be regulated. Some regulators classify digital assets as securities (Phillips, 2021), while others classify them as commodities or currencies (Peerce et al., 2022). It has important implications for how these assets are taxed and regulated. Another challenge facing regulators is ensuring the security and stability of virtual economies. Virtual economies can be subject to fluctuations and market manipulations, which can have real-world consequences for those who participate in these economies. Therefore, regulators must balance the need for stability and security with the desire to foster innovation and economic growth (Adrian & Mancini-Griffoli, 2021).

The regulation of virtual economies also raises questions about the jurisdiction and sovereignty of virtual states and jurisdictions (Chatham House, 2019). It is because virtual currencies and assets are only sometimes legal tenders in any one jurisdiction, and no coherent international legal framework exists for defining virtual property. Some virtual states have economies and currencies, which may have different norms and values than the real world. Regulators must determine how these virtual states and jurisdictions fit into the existing legal and regulatory framework (The White House, 2022; Ehrentraud et al., 2022) and how they can be held accountable for their activities placed within their borders.

The Legal Implications of Virtual Sovereignty

Virtual sovereignty is the concept of a state or entity controlling its digital data, including customer and employee data, software, hardware, and other digital assets (Kergaravat, 2022). It is closely correlated to the direction of non-intervention. Also, the principles, of prohibiting the threat or use of force for instance, companies have an average of 17 apps leveraging customer data alone. Ensuring compliance across each of those apps and any employee data tech is complex. Consider that 92% of the Western world's data is housed in the US, where the laws often conflict with European laws, and that task compounds in complexity exponentially (Fleming, 2021). It creates a complex situation that is difficult to navigate. The EU is taking steps toward digital sovereignty to address this issue (Amaro, 2019).

The legal implications of virtual sovereignty are complex and vary depending on the situation. Generally speaking, malicious cyber operations can be considered a violation of territorial sovereignty if they cause significant effects in another state (Moynihan, 2019; Kelton et al., 2022). However, activities causing negligible or de minimis effects would not violate territorial sovereignty regardless of whether they are conducted remotely or through physical presence on the affected territory (Moynihan, 2019). Additionally, states have exclusive authority over cyberspace's physical, human, and immaterial (logical or software-related) aspects within their borders (Schmitt, 2017).

The Ethics of Virtual Sovereignty and Control

The ethics of virtual sovereignty and control refer to the moral and philosophical questions that arise in the context of virtual reality environments and online games. These issues include questions about the production, access, and control of information and concerns about environmental harm and ethical use of AI (Bird et al., 2020). Ethical issues could also emerge with the widespread adoption of virtual and augmented reality technology (Slater et al., 2020). Virtual sovereignty refers to sovereignty within virtual reality environments and online games. Control refers to the ability of states and other actors to regulate and shape these environments.

One of the key ethical questions in virtual sovereignty and control is the extent to which virtual states and jurisdictions should be recognized and treated as independent entities with the ability to exercise sovereignty. This question is relevant to developing virtual reality technologies (Slater et al., 2020; Dwivedi et al., 2022) and artificial intelligence (Bird et al., 2020; Bossmann, 2016). Virtual states and jurisdictions may have their norms, values, and economies, raising questions about the extent to which they should be treated as separate and distinct entities. Another important ethical question is how states and other actors should be able to regulate and control virtual reality environments and online games. Virtual reality environments can have real-world consequences, and they can be used for various purposes, including political activism, social networking, and commerce (Flavian et al., 2019). Research has shown that high levels of involvement in social virtual reality games by socially isolated users with low self-esteem can negatively affect their well-being (Lee et al., 2021b). Virtual reality also poses health risks to all ages, including children, who may be especially vulnerable (Kaimara, et al., 2021). Therefore, regulators must ensure that they balance the need to protect the rights and interests of participants in these environments with the need to maintain control and stability.

Protecting personal data and privacy is another important ethical consideration in virtual sovereignty and control (Hummel et al., 2021; Bormida, 2021). Technology has made it easier to collect, store, and share data, which can be used for various purposes. Data privacy protection is necessary to ensure individuals have control over their identity-relevant private data (Ishmaev, 2021). Virtual reality environments often require the collection and use of personal data, which can be subject to theft, misuse, and other security risks (Dick, 2021). These risks include exposing users to significant personal and reputational harm and privacy concerns that have yet to be fully addressed (Hunter, 2022). Therefore, regulators must ensure that virtual reality environments are subject to appropriate privacy protections and that people's data is secure.

The Influence of Social Media Platforms on Nation-State Sovereignty

Social media has transformed the way people communicate and interact with one another, as well as the way governments operate. With the rise of social media platforms, it has become more accessible for people to connect, share information, and organize themselves around a common cause. However, this has also raised concerns about the impact of social media on nation-state sovereignty, as social media can challenge the power and authority of governments.

One of how social media can influence nation-state sovereignty is through its ability to facilitate the spread of information and ideas (Makarychev & Yasick, 2018). It can alter civic engagement and affect political systems (Jones & Trice, 2020). However, some argue that the internet and social media can strengthen national and global governance (Perritt, 1998). Social media platforms such as Twitter, Facebook, and Instagram give people a powerful tool for expressing their opinions and sharing information. It can lead to the emergence of new political movements and the mobilization of people around a common cause. For example, the Arab Spring protests that swept the Middle East in 2011 were primarily organized and mobilized through social media. Social media platforms such as Facebook and Twitter played a significant role in the protests, with young protesters using these platforms to organize and mobilize people to take to the streets (Brown et al., 2012; Hassan, 2015; Clarke & Kocak, 2020). The Arab Spring was a series of anti-government protests, uprisings, and armed rebellions that spread across much of the Arab world (Britannica, 2023).

However, the power of social media to influence nation-state sovereignty is not limited to its ability to facilitate the spread of information and ideas. Social media can also undermine governments' authority, particularly in authoritarian regimes. Social media platforms can intensify the power of solid authoritarian regimes by helping them, directly or indirectly, to become "digital authoritarianism" (Schleffer & Miller, 2021). By providing people with a platform for expressing their opinions and organizing themselves, social media can challenge the legitimacy of governments and erode their control over society. It has led many governments to restrict access to social media platforms or monitor and censor content on these platforms. Some countries have asked social media companies to remove objectionable content (Siripurapu & Merrow, 2012), while others have imposed outright bans on social media.

Another way social media can influence nation-state sovereignty is through its ability to facilitate the spread of misinformation and propaganda (OECD, 2022). It can lead to polarized public opinion, violent extremism, and hate speech (Council of Europe, n d). Social media platforms can be used to spread false information, conspiracy theories, and propaganda, which can undermine the credibility of governments and institutions. It has become particularly apparent in recent years, as social media has been used to spread disinformation about elections, public health issues, and other important events. The political effects of social media platforms on different countries can also vary depending on the level of state control over its sovereign territory (Schleffer & Miller, 2021).

Issues of State over Social Media Platform (Tiktok)

USA

TikTok is a social media platform that allows users to create and share short videos with their followers. It has become prevalent worldwide, with over 1 billion monthly active users as of early 2022 (Geyser, 2022). The app is available in over 150 countries and has been downloaded over 210 million times in the United States alone (Wallaroo, 2023). However, the platform has faced significant scrutiny and controversy in the United States. The main issue with TikTok in the United States is its ownership by the Chinese company ByteDance. It has raised concerns about data privacy and national security. There are fears that the Chinese government could access and use data from TikTok to spy on or influence American citizens (Fung, 2023). In response to these concerns, former President Donald Trump issued an executive order in August 2020 that would have banned TikTok in the United States unless it was sold to an American company. The order cited national security concerns and gave TikTok 45 days to find a buyer. However, a federal judge ultimately blocked the order, and TikTok remained operational in the United States.

Despite this, TikTok has faced scrutiny from lawmakers and regulators in the United States due to security risks raised over its Chinese-based parent company (Klar & Kagubare, 2023). In December 2020, the Federal Trade Commission (FTC) fined TikTok $5.7 million for illegally collecting personal information from children under 13 (Timberg & Romm, 2019). TikTok has also faced accusations of censorship and bias in its content moderation practices. In response to these issues, TikTok has addressed concerns about data privacy and security. It has hired American executives and established a separate entity, TikTok Global, to manage its operations in the United States (Perault & Sacks, 2023). TikTok has also promised to store American user data in the United States and to provide transparency in its data handling practices (Wang & Shepardson, 2022).

China

One of the main concerns about TikTok is its ties to China and the Chinese government. The company have been allegations that the Chinese government has access to user data collected by TikTok (Hadero, 2023). It has raised concerns about user privacy and the potential for the Chinese government to use TikTok to spread propaganda or censor content (Rodriguez, 2021). Another issue with TikTok is its content moderation policies. Critics have accused TikTok of censoring content that is critical of the Chinese government, or that deals with sensitive topics like the protests in Hong Kong or the treatment of Uyghur Muslims in China. TikTok has denied these allegations, but the company has also faced criticism for its algorithmic recommendation system, which has been accused of promoting harmful or misleading content.

In response to these concerns, TikTok has taken steps to address its relationship with China and to improve its content moderation policies. The company has said that it stores user data in the United States and Singapore and has hired outside auditors to review its content moderation policies (Molla, 2021). TikTok has also announced plans to open a "transparency center" in the United States, where outside experts can review its source code and data handling practices (TikTok, 2020). TikTok has also implemented new content moderation policies to address concerns about spreading misinformation and propaganda on its platform. The company has increased its use of fact-checking tools and is partnering with third-party fact-checkers to help identify and remove false information (TikTok, 2021). These steps taken by TikTok are part of an effort to regain the trust of its users and address concerns about privacy and content moderation. However, some experts argue that more needs to be done, including greater transparency about how user data is collected and used (Baldwin, 2021).

England

Concerns have been raised about TikTok's impact on young people in England and the potential for the platform to spread harmful content. One of the main concerns about TikTok in England is its impact on young people's mental health. A study by the Royal Society for Public Health found that social media platforms, including TikTok, can harm young people's mental health by increasing anxiety, depression, and poor body image (Royal Society for Public Health, 2019). Additionally, concerns have been raised about the potential for spreading harmful content, including disinformation; hate speech, and bullying, on TikTok. The UK government has called on social media platforms, including TikTok, to do more to tackle harmful content and protect users, particularly young people (UK Department for Digital, Culture, Media & Sport, 2021). In response to these concerns, the UK government has taken steps to regulate social media platforms, including TikTok. In April 2021, the government announced plans to introduce a new Online Safety Bill, which would give Ofcom, the UK's media regulator, the power to fine social media companies up to 10% of their global revenue if they fail to remove harmful content from their platforms (Department for Digital, Culture, Media & Sport, 2021). Additionally, the government has called on social media companies to take greater responsibility for their platforms' content and do more to protect young people (Department for Digital, Culture, Media & Sport, 2019).

Another issue with TikTok in England is its relationship with the Chinese-owned parent company, ByteDance. The UK government has raised concerns about the potential for the Chinese government to access user data collected by TikTok and has called on the company to be more transparent about its data handling practices (BBC News, 2021). Additionally, concerns have been raised about the potential for TikTok to be used to spread disinformation and propaganda. In response to these concerns, TikTok has taken steps to address its relationship with China and to improve its content moderation policies. The company has said it stores user data in the United States and other countries outside of China and has committed to providing greater transparency about its data handling practices. TikTok has also introduced new tools and policies to help users identify and report harmful content, including disinformation and hate speech.

METHODS

This study investigates the available literature on technology and metaverse on traditional absolute sovereignty control of modern national states territories using the concept of "virtual sovereignty." Virtual sovereignty refers to the ability of entities, including individuals and organizations, to exercise a degree of control over virtual spaces and resources within the metaverse, which can potentially challenge the traditional concept of state sovereignty. The rise of technology and the metaverse may empower individuals and organizations to exert more significant influence and control over virtual spaces, potentially leading to conflicts with state authorities. Therefore, virtual sovereignty may help understand the metaverse's evolving relationship between technology and state sovereignty.

In strengthening the discussion, the results of former studies have been used. As a theoretical article paper, the methodology will contain an assessment of secondary data from different resources such as published research papers, reports, theses, and conference proceeding papers to boost the overall effectiveness of the research and elucidate the existing ideas (Dawadi et al., 2021). The rationale of why academic researchers use secondary research methods is because of their cost-effectiveness. Since only some organizations can settle a sizeable amount of money for the research, they utilize secondary data sources and organize them for analysis. Hence, secondary research is "desk research," as the data may be available while behind a desk.

RESULTS AND DISCUSSION

The rise of technology and the development of a metaverse (a virtual shared space) can challenge traditional absolute sovereignty control of modern national state territories. It can occur in several ways:

Borderless Access

The ability to access virtual spaces and experiences without being restricted by physical borders or geographical location is called the metaverse (Dwivedi et al., 2022). The metaverse is a virtual expanse outside the confines of everyday life, a universe beyond real life (Hooijdonk, 2021). It will encompass infinite virtual spaces inside other virtual spaces, including any environment. Users will be able to jump in and out of this parallel world, which will ultimately free us from any physical limitations.

The digital divide refers to the gap between demographics and regions with access to current information and communications technology (ICT) and those without limited entry. This technology can include television, telephone, internet, and personal computers. Globally, developing countries need access to digital technology and internet service. There is also a significant imbalance across the sphere of telecommunication bandwidth. For example, Venezuela and Paraguay feature some of the lowest digital access speeds, followed by Egypt, Yemen, and Gabon (Hanna, n.d). The concept of borderless access has significant implications for nations and their ability to control their borders and regulate the flow of people and goods (Stanford Graduate School of Business, 2004). The Schengen Area is an example of a borderless area in Europe that guarantees free movement to EU citizens. However, nations are increasingly attempting to control data produced within their perimeters, disrupting the flow of information across borders (McCabe & Satariano, 2022). Border policing has high symbolic and perceptual value as an instrument of territorial exclusion (Andreas, 2003).

With the ability to access virtual spaces and experiences, people are no longer limited by physical borders (International Labor Organization, 2020), making it more difficult for governments to monitor and control their movements (National Intelligence Council, 2012). It has been highlighted during the COVID-19 pandemic, which has seen an increase in teleworking and other forms of remote work. Blockchain technology is also being explored to facilitate secure transactions across borders (CB Insights, 2022), further complicating government efforts to regulate movement. Physical activity guidelines have also been developed to help individuals make healthy choices for themselves and their families (U.S. Department of Health and Human Services, 2018). Additionally, virtual transactions and interactions can also pose challenges to regulators in taxing and tracking the flow of goods and services, making it difficult for nations to enforce their laws and regulations. Regulators have begun to address these challenges with various approaches across countries (He et al., 2016). The digital economy also challenges value-added tax collection (OECD, 2015). There is a debate over whether digital platforms should be regulated (Simpson & Conner, 2021). The Financial Action Task Force has issued guidance on virtual assets and service providers (Financial Action Task Force, 2021).

The benefits of borderless access also include increased accessibility and opportunities for people from around the world to connect, collaborate and transact with each other (Meltzer, 2014). It can reduce real estate costs, global talent acquisition, and other benefits for organizations (Choudhury, 2020). However, it may also raise unexpected issues that have different impacts on institutions in countries of varying degrees (Henard et al., 2012). The metaverse is another example of a 3D virtual shared world where people can connect and interact with each other regardless of physical location (Dwivedi et al., 2022). It can also provide a platform for international trade and commerce to facilitate the exchange of ideas and knowledge (Lopez-Gonzalez, 2021). Overall, borderless access can transform how people interact and transact with each other globally. However, it raises important questions about how nations can regulate and control these interactions.

Jurisdictional Disputes

Conflicts arising from the challenges posed by the metaverse to existing legal and regulatory frameworks of nation-states refer to governance challenges related to the applicability of national laws, policies, issues of consent, and the rule of law (Dwivedi et al., 2022). Experts have expressed concerns that large-scale virtual platforms and immersive environments could pose regulatory issues (Zhu, 2022). There is a need for an ex-ante regulatory framework that upholds user welfare and civil rights in implementing the metaverse (De Asua et al., 2022). As a result, disputes may arise over who has the authority and jurisdiction to regulate activity in the metaverse.

For instance, it may be unclear in the virtual world which country has jurisdiction over a particular transaction or activity or the regulation of virtual goods and services (He et al., 2016). Blockchain technology is decentralized, and there is no central governance (Copeman et al., 2022). However, some countries have created regulations to address these issues (European Banking Authority, 2014; Commerce Department, 2021). This lack of clarity can lead to disputes over which country has the authority to enforce its laws and regulations in the metaverse. Additionally, the virtual nature of the metaverse may make it difficult for authorities to enforce their laws and regulations effectively, leading to further challenges in resolving these disputes.

It will address these challenges, new laws and regulations may need to be created, or existing ones may need to be adapted to regulate the metaverse (Londoño, 2022; Ramos, 2022). Some argue that existing laws are not adapted to the metaverse environment, while others suggest that traditional financial regulations such as commodities, banking, and securities laws apply (Blockchain Council, 2023). Privacy standards in the metaverse are also a concern (Phillips et al., 2023). It can require international cooperation and coordination among nations to ensure a harmonized legal framework for the metaverse. Also, it can help prevent and resolve jurisdictional disputes.

Decentralization of Power

The decentralized nature of the metaverse, built on technologies like blockchain, can disrupt the centralized control of national governments. In a decentralized system, power is distributed among multiple actors rather than being centralized in the hands of a single entity (Portincaso, 2022; Deer, 2022). It can be contrasted with centralized systems, where control is held by one authority. Decentralization is often associated with blockchain technology and other distributed networks (Vergne, 2020). In the context of the metaverse, this could mean that individuals and communities have greater control over their data, assets, and identity rather than having it controlled by a single authority. In a decentralized system, transactions and interactions are recorded on a public ledger, maintained by a network of users rather than a central authority. It permits excellent accountability and transparency, as the ledger is difficult to manipulate or alter. In the metaverse, this could lead to a shift in power from governments to individuals and communities, as individuals have more control over their personal information, assets, and online identity (Wells, 2022).

However, decentralizing power also raises questions about regulation, security, and accountability in the metaverse (Tusk, 2022; Wells, 2022; Poskonoff, 2023). For example, it may be more difficult to enforce laws and regulations, as the decentralized nature of the metaverse makes it harder to track and regulate activity. It is especially true in a fully decentralized world where governments hold no citizen data (Caserta, 2023). The metaverse will bring multiple new legal implications, especially without existing standards and precedence (Kumar, 2022). Existing laws may prove insufficient to address problematic conduct, which might trigger the passage of new laws and regulations (Ara et al., 2022). Additionally, decentralizing power could lead to new security challenges, as individuals and communities are more responsible for their own data and assets.

Overall, the decentralization of power in the metaverse represents opportunities and challenges for individuals, communities, and governments. While it has the potential to give individuals greater control over their data, assets, and identity, it also raises questions about regulation, security, and accountability.

Cyber security Concerns

The metaverse is a virtual environment where people connect, interact, and shop. As the metaverse takes shape, companies must consider new cyber security challenges and how to deal with them. The foundation of the metaverse needs to be underpinned by security for reasons such as reputation (Krishnan, 2022). The success of the metaverse depends on its ability to provide a safe and secure environment for users. However, there are concerns that the metaverse may bring new cyber risks (Ong, 2022). One primary concern is data breaches. As users leave data trails around the metaverse, this problem in the real world may also cross into virtual reality. In immersive worlds, new technologies will siphon up data at an increasingly granular level, such as a person's gait, eye movements, and emotions putting far more significant strain on existing safeguards. Government or technology companies and researchers are beginning to wonder whether the metaverse will be any different from current forms of data collection that some critics liken to mass surveillance (Uberti, 2022).

The safety, privacy, and well-being of potentially billions of users are at stake in the metaverse. Since users will own their personal data and digital assets in the metaverse, regulators will be keen to ensure users are in control and established regulatory principles transfer appropriately to new interactions and transactions. Policymakers will avoid mistakes made during the web 2.0 eras, where regulatory safeguards were implemented late and reactively (GSMA, 2023). Governments or companies must address privacy and security issues when adopting the metaverse. They must consider cybersecurity risks, such as data breaches and privacy issues that this new virtual universe might contain (Krishnan, n.d). Key mitigating actions must be taken to prevent potentially amplified risks in the metaverse (Deloitte, 2022). Additionally, national governments may need to collaborate with international organizations and other countries to develop effective strategies to address the evolving cybersecurity challenges the metaverse poses.

Conceptual Framework

In the traditional absolute sovereignty model of modern national state territories, a state has complete control over its borders, jurisdiction, and power. However, several factors have emerged (as seen in Figure 1) in recent years that challenge this model and the state's control over its territory.

Borderless access refers to the ease with which people, goods, and information can cross national borders. The development of technology, such as the internet and social media, has made it easier for people to connect and communicate across borders, often bypassing traditional government controls. It undermines the conventional idea of territorial control, as the state's ability to regulate what happens within its borders is eroded.

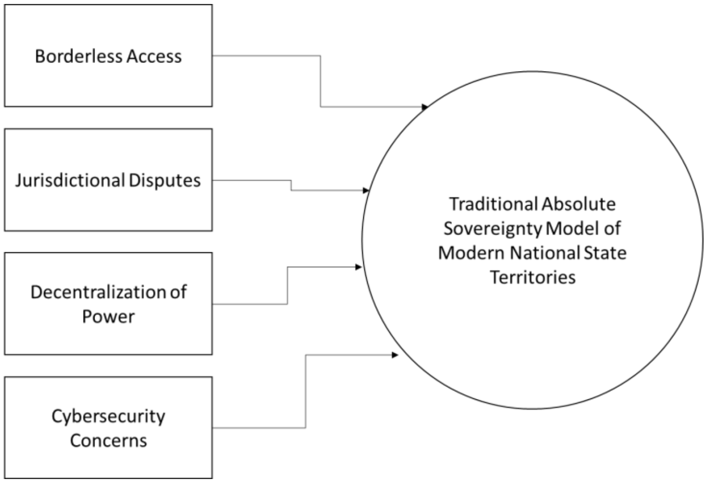
Borderless Access
Jurisdictional Disputes
Decentralization of Power
Cybersecurity Concerns
Traditional Absolute Sovereignty Model of Modern National State Territories

Figure 1. Conceptual Framework

Jurisdictional disputes arise when multiple states claim authority over the same territory or issue. In some cases, such arguments can lead to conflicts between states. These disputes can also create gaps in the state's control over its territory, as other states or international organizations may become involved in resolving the issue.

Decentralization of power refers to devolving power and decision-making authority away from central governments and towards regional or local governments. It can undermine the state's ability to control its territory, as power is distributed among multiple levels of government. Decentralization can also create opportunities for regional or local governments to challenge the central government's authority.

Finally, cyber security concerns arise from the increasing importance of technology in modern life. Using the internet and other digital technologies creates vulnerabilities that hackers, cybercriminals, and other malicious actors can exploit. It undermines the state's ability to control what happens within its borders, as threats can originate from outside the territory.

In summary, borderless access, jurisdictional disputes, decentralization of power, and cyber security concerns all challenge modern national state territories' traditional absolute sovereignty model. These factors undermine the state's control over its borders, jurisdiction, and power, creating new challenges for governments to maintain order and stability within their territories.

CONCLUSION

The metaverse raises severe concerns regarding determinism. Due to the problematic nature of the metaverse in terms of its inherent ethical and social implications, there is a need to establish morally acceptable and collectively most democratically beneficial rules for society (Bibri, 2022).

The metaverse is envisioned as a version of the internet with three-dimensional virtual environments that may support entertainment, shopping, education, communication, and work environments in one seamless space. However, whose rules would apply because there would be no national boundaries in the metaverse? What laws concerning privacy and consumer product? The answer lies in “meta jurisdiction” for global rules that many stakeholders, not just states, could enforce. Technologists, nongovernmental organizations, and lawyers must work shoulder to shoulder to ensure that nefarious actors or self-interested states do not stymie the internet’s full potential or bind it by traditional notions of the jurisdiction (Cooper, 2021).

Economic globalization and technology have brought significant transformations in the authority of national states. Significant here is the growth of new non-state-centered governance mechanisms, which have transformed the meaning of national territorial sovereignty independently from whatever impact the internet has had. The growth of digitalized global financial markets can deploy considerable power against the will of national states (Sassen, 1999). If Central Bank Digital Currencies are used in cross-border payments, their influence goes quickly beyond national territory.

FUTURE IMPLICATIONS

The metaverse is a virtual world that is expected to impact state sovereignty in the future significantly. As the metaverse gains commercial interest by attracting users and money, many issues that need to be managed across virtual environments with potentially billions of users will require new legal frameworks. Governments will be forced to act and create legal frameworks that cover everything in the Metaverse (Diwakar, 2022). The link between industry and government interests is represented in how governments are concerned with the strategic impact on interstate competition and potential risks to their internal political and social spheres (Vanorio, 2022).

The metaverse raises the matter of sovereignty and the possibility of states existing in it. Countries with limited resources in the real world now hold the potential to position themselves as attractive jurisdictions in the metaverse. Small nations lacking natural resources could compete with new sovereign players in the metaverse. Citizenships in the Metaverse are bound to democratize resource distribution among nation-states, driving new benchmarks of democracy and eradicating the current political polarization (Handa, 2022).

The metaverse's potential use of decentralized ownership using technologies could cause political and technical changes. Zuckerberg envisions decentralized ownership using blockchain technology for self-sovereignty in the metaverse. People establishing presences in the metaverse may someday pursue sovereignty and virtual jurisdiction. While some concepts of sovereignty would require changes in law, other aspects of virtual spaces obtaining self-sovereignty and virtual jurisdiction were especially intriguing as long-term possibilities (Westby, 2022).

REFERENCES

Andreas, P. (2003). Redrawing the Line: Borders and Security in the Twenty-First Century. International Security, 28(2), 78-111. https://www.jstor.org/stable/4137469

Adrian, T. & Mancini-Griffoli, T. (2021). A New Era of Digital Money. Finance and Development. Retrieved from https://www.imf.org/external/pubs/ft/fandd/2021/06/online/digital-money-new-era-adrian-mancini-griffoli.htm

Ahi, A. A., Sinkovics, N., Shildibekov, Y., Sinkovics, R. R. & Mehandjiev, N. (2022). Advanced technologies and international business: A multidisciplinary analysis of the literature. International Business Review, 31(4), 101967. https://doi.org/10.1016/j.ibusrev.2021.101967

Amaro, S. (2019 November 20). Europe's dream to claim its 'digital sovereignty' could be the next big challenge for US tech giants. Retrieved from https://www.cnbc.com/2019/11/20/us-tech-could-face-new-hurdles-as-europe-considers-digital-sovereignty.html

Ara, T., Radcliffe, M., Fluhr, M. & Imp, K. (2022). Exploring the metaverse: What laws will apply? Retrieved from https://www.dlapiper.com/en/insights/publications/2022/02/exploring-the-metaverse

Artz, M. (2022). Metaverse and Privacy. https://iapp.org/news/a/metaverse-and-privacy-2/

Baldwin, C. (2021, February 10). TikTok's security and transparency still fall short, experts say. Reuters. https://www.reuters.com/article/us-tiktok-security/tiktoks-security-and-transparency-still-fall-short-experts-say-idUSKBN2AB0AA

Balkin, J. (2017). The Three Laws of Robotics in the Age of Big Data. Information Technology and Systems eJournal.

Ball, M. (2020). The Metaverse: What It Is, Where to Find it, and Who Will Build It. https://www.matthewball.vc/all/themetaverse

BBC News. (2021, February 15). TikTok faces UK investigation over children's privacy. https://www.bbc.com/news/technology-56016332

Bellanova, R., Carrapico, H. & Duez, D. (2022). Digital/sovereignty and European Security Integration: An Introduction. European Security, 31(3), 337-355. DOI: 10.1080/09662839.2022.2101887

Bibri, S.E. (2022). The Social Shaping of the Metaverse as an Alternative to the Imaginaries of Data-Driven Smart Cities: A Study in Science, Technology, and Society. Smart Cities, 5, 832–874. https://doi.org/10.3390/smartcities5030043

Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Emma Weitkamp, E. & Winfield, A. (2020). The ethics of artificial intelligence: Issues and initiatives. European Parliamentary Research Service.

Blockchain Council (2023 January 16). What Laws Govern the Metaverse? Retrieved from https://www.blockchain-council.org/metaverse/what-laws-govern-the-metaverse/

Bossmann, J. (2016). Top 9 ethical issues in artificial intelligence. Emerging Technologies. Retrieved from https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/

Bormida, M.D. (2021). The Big Data World: Benefits, Threats and Ethical Challenges. Iphofen, R. and O'Mathúna, D. (Ed.) Ethical Issues in Covert, Security and Surveillance Research (Advances in Research Ethics and Integrity, Vol. 8), Emerald Publishing Limited, Bingley, pp. 71-91. https://doi.org/10.1108/S2398-601820210000008007

Britannica, The Editors of Encyclopaedia. "Arab Spring". Encyclopedia Britannica, 14 Feb. 2023, https://www.britannica.com/event/Arab-Spring. Accessed 21 March 2023.

Brookings (2022 November 15). Digital asset regulation: The state perspective Effective regulatory design and implementation for virtual currency. Retrieved from https://www.brookings.edu/events/digital-asset-regulation-the-state-perspective/

Brown, H., Guskin, E. & Mitchell, A. (2012). The Role of social media in the Arab Uprisings. Retrieved from https://www.pewresearch.org/journalism/2012/11/28/role-social-media-arab-uprisings/

Buckler, N. (2022). Phygital World: The Metaverse is Merging our Real and Digital Lives. https://beincrypto.com/phygital-world-the-metaverse-is-merging-our-real-and-digital-lives/

Caserta, R. (2023). The metaverse: Why governments should care. Retrieved from https://kpmg.com/xx/en/blogs/home/posts/2023/01/the-metaverse-why-governments-should-care.html

Casey, M. J. (2021). Why Barbados' Metaverse Embassy Matters. Opinion. Retrieved from https://www.coindesk.com/policy/2021/11/19/why-barbados-metaverse-embassy-matters/

CB Insights (2022). Banking is only the beginning: 65 big industries blockchain could transform. Retrieved from https://www.cbinsights.com/research/industries-disrupted-blockchain/

Chatham House (2019). The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention. Retrieved from https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace

Choudhury, P. (2020). Our Work-from-Anywhere Future. Harvard Business Review. Retrieved from https://hbr.org/2020/11/our-work-from-anywhere-future

Clarke, K., & Kocak, K. (2020). Launching Revolution: Social Media and the Egyptian Uprising's First Movers. British Journal of Political Science, 50(3), 1025-1045. doi:10.1017/S0007123418000194

Commerce Department (2021 January 19). Securing the Information and Communications Technology and Services Supply Chain, 4909-4928.

Copeman, A., Marsden, J. & Caunt, S. (2022 November 9). Governing law and jurisdiction in the Metaverse under Law Commission review. https://www.dentons.com/en/insights/articles/2022/november/9/governing-law-and-jurisdiction

Cooper, J. (2021, December 2). Why we need 'meta jurisdiction' for the metaverse. Retrieved from https://thehill.com/opinion/technology/583529-why-we-need-meta-jurisdiction-for-the-metaverse/

Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-Methods Research: A Discussion on its Types, Challenges, and Criticisms. Journal of Practical Studies in Education, 2(2), 25-36. DOI: https://doi.org/10.46809/jpse.v2i2.20

Deer, M. (2022 June 11). Centralized vs. decentralized digital networks: Key differences. Retrieved from https://cointelegraph.com/explained/centralized-vs-decentralized-digital-networks-key-differences

Deloitte (2022 April 28). Welcome to the Metaverse: An Avatars Guide to the Health Care Galaxy. Retrieved from https://www2.deloitte.com/

Department for Digital, Culture, Media & Sport. (2019, April 8). Government sets out world-leading plan to keep children safe online. https://www.gov.uk/government/news/government-sets-out-world-leading-plan-to-keep-children-safe-online

Department for Digital, Culture, Media & Sport. (2021, February 15). Government calls for action to tackle harmful online content. https://www.gov.uk/government/news/government-calls-for-action-to-tackle-harmful-online-content

Desir, A. M. (2022 August 30). How effective regulation unlocks the potential of the virtual assets economy. Retrieved from https://www.ey.com/en_us/bbc/how-effective-regulation-unlocks-the-potential-of-the-virtual-assets-economy

De Asua, E. M., Otter, V., Tsukuda, T. & Vivenot, B. (2022). The Metaverse: Challenges and Regulatory Issues (Thesis Master). SciencesPo.

Dick, E. (2021 March 4). Balancing User Privacy and Innovation in Augmented and Virtual Reality. Retrieved from https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/

Diwakar, A. (2022 May 13). The Metaverse will 'become embroiled in future geopolitical conflict'. Retrieved from https://www.trtworld.com/magazine/the-metaverse-will-become-embroiled-in-future-geopolitical-conflict-57118

Downs, K. (2022). What is the Metaverse and How Does it Work? Retrieved from https://blog.servermania.com/what-is-metaverse/

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., Janssen, M. & Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 66, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Edler, J., Blind, K., Kroll, H., Schubert, T. (2021). Technology sovereignty as an emerging frame for innovation policy: Defining rationales, ends and means, Fraunhofer ISI Discussion Papers - Innovation Systems and Policy Analysis, No. 70, Fraunhofer-Institut für System- und Innovations for schung ISI, Karlsruhe

Ehrentraud, J., Evans, J. L., Monteil A. & Restoy, F. (2022). Big tech regulation: in search of a new framework. Occasional Paper No. 20

European Banking Authority (2014). EBA Opinion on 'virtual currencies. Retrieved from https://www.eba.europa.eu/

Financial Action Task Force (2021 October). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris. www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html

Flavian, C., Ibáñez-Sánchez, S. & Orus, C. (2019). The impact of virtual, augmented and mixed reality technologies on the customer experience. Journal of Business Research, 100: 547-560. https://doi.org/10.1016/j.jbusres.2018.10.050

Fleming, S. (2021 March 15). What is digital sovereignty and why is Europe so interested in it? Retrieved from https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/

Fung, B. (2023 March 21). Lawmakers say TikTok is a national security threat, but evidence remains unclear. Retrieved from https://edition.cnn.com/2023/03/21/tech/tiktok-national-security-concerns/index.html

Geyser, W. (2022 December 30). What Is TikTok? – Everything You Need to Know in 2023. Retrieved from https://influencermarketinghub.com/what-is-tiktok/

Greenwald, M. E. (2022). Harnessing the Metaverse: States of All Sizes. Retrieved from https://www.wilsoncenter.org/article/harnessing-metaverse-states-all-sizes

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

Hadero, H. (2023 March 17). Why TikTok's security risks keep raising fears. The New York Times. Retrieved from https://apnews.com/article/tiktok-ban-bytedance-china-biden-administration-14ef5f93dc2114e4ade110b2e85433fd

Handa, N. (2022 September 19). The Future of Residence and Citizenship — Sovereign States in the Metaverse? Retrieved from https://www.hubbis.com/article/the-future-of-residence-and-citizenship-sovereign-states-in-the-metaverse

Hanna, K. T. (n.d.). digital divide. Retrieved from https://www.techtarget.com/whatis/definition/digital-divide

Hassan, S. F. (2015). Social Media And The Arab Spring (Master thesis). Rutgers, The State University of New Jersey.

He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., Kyriakos-Saad, N., Oura, H., Sedik, T. S., Stetsenko, N. and Verdugo-Yepes, C. (2016). Virtual Currencies and Beyond: Initial Considerations. International Monetary Fund.

Henard, F., Leslie Diamond, L. Deborah Roseveare, D. (2012). Approaches to Internationalisation

and Their Implications for Strategic Management and Institutional Practice: A Guide for Higher Education Institutions.

Hummel, P., Braun, M., Tretter, M. & Peter Dabrock, P. (2021). Data sovereignty: A review. Big Data & Society, 8:1. https://doi.org/10.1177/2053951720982012

Hunter, T. (2022 January 13). Surveillance will follow us into 'the metaverse,' and our bodies could be its new data source. Retrieved from https://www.washingtonpost.com/technology/2022/01/13/privacy-vr-metaverse/

Hooijdonk, R. (2021). The metaverse: blurring the lines between our physical and virtual worlds. Retrieved from https://blog.richardvanhooijdonk.com/en/the-metaverse-blurring-the-lines-between-our-physical-and-virtual-worlds/

International Labour Organization (2020). Teleworking during the COVID-19 pandemic and beyond: A Practical Guide.

Ishmaev, G. (2021). Sovereignty, privacy, and ethics in blockchain-based identity management systems. Ethics and Information Technology, 23, 239-252. https://doi.org/10.1007/s10676-020-09563-x

Jon M. Garon, J. M. (2022). Legal Implications of a Ubiquitous Metaverse and a Web3 Future. Marquette Law Review, 163(1), 163-242. Available at: https://scholarship.law.marquette.edu/mulr/vol106/iss1/5

Jones, J. & Trice, M. (2020). Social Media Effects: Hijacking Democracy and Civility in Civic Engagement. Platforms, Protests, and the Challenge of Networked Democracy, 77-94. DOI: 10.1007/978-3-030-36525-7_5

Joshua, J. (2017). Information Bodies: Computational Anxiety in Neal Stephenson's Snow Crash. Interdisciplinary Literary Studies, 19 (1): 17-47. https://doi.org/10.5325/intelitestud.19.1.0017

Kaimara, P., Oikonomou, A. & Deliyannis, I. (2022). Could virtual reality applications pose real risks to children and adolescents? A systematic review of ethical issues and concerns. Virtual Reality, 26, 697–735. https://doi.org/10.1007/s10055-021-00563-w

Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E. & Troath, S. (2022). Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States, International Affairs, 98(6), 1977-1999. https://doi.org/10.1093/ia/iiac226

Kergaravat, C. (2022 November 25). Everything You Need to Know About Digital Sovereignty. Retrieved from https://www.apizee.com/digital-sovereignty/

Klar, R. & Kagubare, I. (2023 March 21). Why pressure is building to ban TikTok. Retrieved from https://thehill.com/policy/technology/3908720-why-pressure-is-building-to-ban-tiktok/

Krishnan, A. (2022 November 18). Top metaverse cybersecurity challenges: How to address them. Retrieved from https://www.techtarget.com/searchsecurity/tip/Top-metaverse-cybersecurity-challenges-to-consider

Kumar. N. (2022). Six Unaddressed Legal Concerns for The Metaverse. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2022/02/17/six-unaddressed-legal-concerns-for-the-metaverse/?sh=4c9a750b7a94

Lauer, D. (2021). Facebook's ethical failures are not accidental; they are part of the business model. AI and Ethics, 1, 395-403. https://doi.org/10.1007/s43681-021-00068-x

Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z. & Hui, P. (2021a). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. arXiv, 2110: 05352. https://doi.org/10.48550/arXiv.2110.05352

Lee H-W, Kim S and Uhm J-P (2021b). Social Virtual Reality (VR) Involvement Affects Depression When Social Connectedness and Self-Esteem Are Low: A Moderated Mediation on Well-Being. Frontiers in Psychology, 12:753019. doi: 10.3389/fpsyg.2021.753019

Londoño, J. (2022 February 9). Will Metaverses Require New Regulations? Insight. Retrieved from https://www.americanactionforum.org/insight/will-metaverses-require-new-regulations/

Lopez-Gonzalez, J. (2021 April 21). The changing nature of digital trade, current and future barriers and ideas to overcome them. Insight and Analysis. Retrieved from https://www.wilsoncenter.org/article/changing-nature-digital-trade-current-and-future-barriers-and-ideas-overcome-them

Makarychev, A., & Yatsyk, A. (2018). Social media and the transformation of nation-state sovereignty. International Journal of Politics, Culture, and Society, 31(3), 229-246. doi: 10.1007/s10767-017-9279-x

McCabe, D. & Satariano, A. (2022). The Era of Borderless Data Is Ending. Retrieved from https://www.nytimes.com/2022/05/23/technology/data-privacy-laws.html

Meltzer, J. P. (2014). The Internet, Cross-Border Data Flows and International Trade. Asia and The Pacific Policy Studies, 2(1), 90-102. https://doi.org/10.1002/app5.60

Mileva, G. (2023, January 23). The State of the Metaverse 2023 | Challenges & Opportunities. Retrieved from https://influencermarketinghub.com/state-of-the-metaverse/

Molla, R. (2021, January 29). What TikTok's sale means for its future, and its users. Vox. https://www.vox.com/recode/22252009/tiktok-deal-sale-microsoft-walmart-trump-ban

National Intelligence Council (2012). Global Trends 2030: Alternative Worlds.

Newton, C. (2021). Mark in the Metaverse. https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview

OECD (2015), Addressing the Tax Challenges of the Digital Economy, Action 1 - 2015 Final Report, OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264241046-en

OECD (2022 November 3). Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses. Retrieved from https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/

Ong, C. (2022 March 22). The metaverse may bring new cyber risks. Here's what companies can do. Retrieved from https://www.cnbc.com/2022/03/23/the-metaverse-may-bring-new-cyber-risks-heres-what-firms-can-do.html

Over (2022). The Building Blocks of a Digital Nation. Retrieved from https://www.overthereality.ai/blog/the-building-blocks-of-a-digital-nation/

Peerce, M. J., Diamond, S. L. & Cobb, T. M. (2022). A Taxonomy of Digital Assets: Is It a Security, Commodity, Banking Product, or Something Else? Retrieved from https://www.ballardspahr.com/Insights/Alerts-and-Articles/2022/10/A-Taxonomy-of-Digital-Assets-Is-It-a-Security-Commodity-Banking-Product-or-Something-Else

Perault, M. & Sacks, S. (2023 January 26). Project Texas: The Details of TikTok's Plan to Remain Operational in the United States. Retrieved from https://www.lawfareblog.com/project-texas-details-tiktoks-plan-remain-operational-united-states

Perritt, H. H. (1998). The Internet as a Threat to Sovereignty? Thoughts on the eignty? Thoughts on the Internet's Role in Strengthening National and Global Governance. Indiana Journal of Global Legal Studies, 5(2), Article 4. Available at: https://www.repository.law.indiana.edu/ijgls/vol5/iss2/4

Phillips, T. (2021 October 4). The SEC's Regulatory Role in the Digital Asset Markets. Retrieved from https://www.americanprogress.org/article/secs-regulatory-role-digital-asset-markets/

Phillips, G., Brachmann, M., Lawson, L. & Tudor, V. (2023 February 17). Privacy standards in the metaverse: An end to the wild west days of innovation? Retrieved from https://www.ericsson.com/en/blog/2023/2/privacy-standards-in-the-metaverse

Portincaso, M. (2022 December 11). Decentralized vs. Distributed - Part II/ Buildings as Power Plants/ Organ-on-a-Chip Revolution/ 1.200 Possible Futures. Retrieved from https://www.linkedin.com/pulse/decentralized-vs-distributed-part-ii-buildings-power-portincaso?trk=pulse-article_more-articles_related-content-card

Poskonoff, K. (2023 February 3). 5 Questions for the Metaverse. Retrieved from https://arinsider.co/2023/02/03/5-questions-for-the-metaverse/

Purdy, M. (2022). How the Metaverse Could Change Work. Harvard Business Review. https://hbr.org/2022/04/how-the-metaverse-could-change-work

Ramos, A. (2022 June). The metaverse, NFTs and IP rights: to regulate or not to regulate?WIPO Magazine. Retrieved from https://www.wipo.int/wipo_magazine/en/2022/02/article_0002.html

Rodriguez, S. (2021 June 25). TikTok insiders say social media company is tightly controlled by Chinese parent ByteDance. Retrieved from https://www.cnbc.com/2021/06/25/tiktok-insiders-say-chinese-parent-bytedance-in-control.html

Royal Society for Public Health. (2019). #StatusOfMind: Social media and young people's mental health and wellbeing. https://www.rsph.org.uk/uploads/assets/uploaded/62b58022-8524-4c87-9a4f9a4f9a4fdddc.pdf

Riddle, J. (2017). All Too Easy: Spreading Information Through Social Media. https://ualr.edu/socialchange/2017/03/01/blog-riddle-social-media/

Rodriguez, S. (2021 June 25). TikTok insiders say social media company is tightly controlled by Chinese parent ByteDance. Retrieved from https://www.cnbc.com/2021/06/25/tiktok-insiders-say-chinese-parent-bytedance-in-control.html

Sassen, S. (1999). The Impact of the Internet on Sovereignty: Real and Unfounded Worries. Information Technology and Tools Global Disclosure Project. https://nautilus.org/information-technology-and-tools/the-impact-of-the-internet-on-sovereignty-real-and-unfounded-worries/

Schleffer, G. & Miller, B. (2021). The Political Effects of Social Media Platforms on Different Regime Types. Media and Democracy, 77-103. http://dx.doi.org/10.26153/tsw/13987

Schmitt, M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.

Shone, G. & Humairah, L. (2022, January 9). New virtual economy: what does the rise of The Metaverse mean? Retrieved from https://www.euronews.com/next/2022/08/17/new-virtual-economy-what-does-the-rise-of-the-metaverse-mean

Simpson, E. & Conner, A. (2021 November 16). How To Regulate Tech: A Technology Policy Framework for Online Services. Retrieved from https://www.americanprogress.org/article/how-to-regulate-tech-a-technology-policy-framework-for-online-services/

Siripurapu, A. & Merrow, W. (2021 February 9). Social Media and Online Speech: How Should Countries Regulate Tech Giants? Retrieved from https://www.cfr.org/in-brief/social-media-and-online-speech-how-should-countries-regulate-tech-giants

Slater M, Gonzalez-Liencres C, Haggard P, Vinkers C, Gregory-Clarke R, Jelley S, Watson Z,

Breen, G., Schwarz, R., Steptoe, W., Szostak, D., Halan, S., Fox, D. & Silver J. (2020) The Ethics of Realism in Virtual and Augmented Reality. Frontiers in Virtual Reality, 1:1. doi: 10.3389/frvir.2020.00001

Stanford Graduate School of Business (2004). Economics Research: What Would Happen if We Removed Borders? Economics. Retrieved from https://www.gsb.stanford.edu/insights/economics-research-what-would-happen-if-we-removed-borders

The Verge (2021). Mark in the Metaverse. Accessed on 23.04.2022. https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview.

The White House (2022 March 9). Executive Order on Ensuring Responsible Development of Digital Assets. Retrieved from https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

TikTok. (2020, May 20). TikTok Announces New Transparency Center as Part of Ongoing Commitment to Transparency [Press release]. https://www.businesswire.com/news/home/20200520005379/en/TikTok-Announces-New-Transparency-Center-as-Part-of-Ongoing-Commitment-to-Transparency

TikTok. (2021, March 2). Fighting Misinformation on TikTok. https://newsroom.tiktok.com/en-us/fighting-misinformation-on-tiktok

Timberg, C. & Romm, T. (2019 February 27). The U.S. government fined the app now known as TikTok $5.7 million for illegally collecting children's data. Retrieved from https://www.washingtonpost.com/technology/2019/02/27/us-government-fined-app-now-known-tiktok-million-illegally-collecting-childrens-data/

Tucci, L. (2022). What is the metaverse? An explanation and in-depth guide. Retrieved from https://www.techtarget.com/whatis/feature/The-metaverse-explained-Everything-you-need-to-know

Tusk, B. (2022 January 31). Regulating the Metaverse(s). retrieved from https://mirror.xyz/0x81dB200eD62Ce664B911C211b55F836a208Df868/n-8osyXEl8Dzv_qnrBR1ICdxF55zdIMLP6OI3yU9igY

Uberti, D. (2022 January 4). Come the Metaverse, Can Privacy Exist? The Wall Street Journal. Retrieved from https://www.wsj.com/articles/come-the-metaverse-can-privacy-exist-11641292206

UK Department for Digital, Culture, Media & Sport. (2021, February 15). Government calls for action to tackle harmful online content. https://www.gov.uk/government/news/government-calls-for-action-to-tackle-harmful-online-content

U.S. Department of Health and Human Services (2018). Physical Activity Guidelines for Americans, 2nd edition. Washington, DC: U.S.

Vanorio, F. (2022 January 2). Metaverse and National Security. Retrieved from https://www.linkedin.com/pulse/metaverse-national-security-fabio-vanorio

Vergne, J. (2020). Decentralized vs. Distributed Organization: Blockchain, Machine Learning and the Future of the Digital Platform. Organization Theory, 1(4). https://doi.org/10.1177/2631787720977052

Wallaroo (2023 March 21). TikTok Statistics – Updated Mar 2023. Retrieved from https://wallaroomedia.com/blog/social-media/tiktok-statistics/

Wang, E. & Shepardson, D. (2022 December 22). Exclusive: TikTok steps up efforts to clinch U.S. security deal. Retrieved from https://www.reuters.com/technology/tiktok-steps-up-efforts-clinch-us-security-deal-2022-12-22/

Wells, L. (2022 May 28). Identity and the Metaverse: Decentralized control. https://cointelegraph.com/news/identity-and-the-metaverse-decentralized-control

Westby, J. (2022 July 19). Self-Sovereignty in the Metaverse. Retrieved from https://www.leadersedge.com/industry/self-sovereignty-in-the-metaverse

Weston, G. (2022). How Does the Metaverse Work? Retrieved from https://101blockchains.com/how-metaverse-works/

Wyss, J. (2021). Barbados Is Opening a Diplomatic Embassy in the Metaverse. https://www.bloomberg.com/news/articles/2021-12-14/barbados-tries-digital-diplomacy-with-planned-metaverse-embassy#xj4y7vzkg

Zhu, L. (2022). The Metaverse: Concepts and Issues for Congress. Congressional Research Service. https://crsreports.congress.gov