GCSP
Geneva Centre for Security Policy

MARCH 2022 | ISSUE 24

Strategic Security Analysis

Our Digital Future: The Security Implications of Metaverses

Jean-Marc Rickli and Federico Mantellassi

www.gcsp.ch

Key Points

- Although the concept of a metaverse or metaverses is not new, current developments in the creation of possible metaverses offer credible prospects of generating increasingly immersive digital experiences that will also provide people with more information, connections and knowledge than ever before.
- However, metaverses are also likely to exacerbate existing risks surrounding the increased digitalisation of our lives and the role of social media companies in our societies, such as the spread of disinformation or increased societal polarisation. Similarly, technology companies' capacity to collect private data and profile users will also increase.
- Growing levels of immersivity will reinforce risks such as increased digital crime or extremist radicalisation, but will also create new ones that pertain to cognitive manipulations. This could lead to the transformation of social organisations and a questioning of the legitimacy of traditional institutions.
- Metaverses also offer new dimensions for power politics and geopolitical confrontations, and a platform for conducting cognitive warfare.
- Responsible innovations and security-by-design must be the guiding principles of efforts to develop metaverses.

About the authors

Dr Jean-Marc Rickli is Head of Global and Emerging Risks as well as of the Polymath Initiative at the GCSP. Among other positions, he is also the co-chair of the Emerging Security Challenges Working Group of the NATO Partnership for Peace Consortium.

Mr Federico Mantellassi is a Research and Project Officer for the Global and Emerging Risks cluster at the GCSP. He is also the project coordinator of the GCSP's Polymath Initiative.

About this publication

This publication is part of a special series of Strategic Security Analysis under the Polymath Initiative supported by the Didier and Martine Primat Foundation. For more information, please visit the Polymath Initiative website: https://www.gcsp.ch/the-polymath-initiative

Introduction

While the *concept* of a metaverse (or metaverses)[1] is not new, interest in the idea has dramatically resurfaced, mainly due to Facebook's headline-grabbing rebranding of itself as "Meta" in October 2021 and its promise to make its proposed Metaverse a 21st century reality. While there have been attempts in the past to build a metaverse, Meta's endeavour is probably the most promising thus far, because the enabling technologies have either matured or are close to maturing, and because of the company's huge allocation of financial and human resources to this project.[2] Additionally, our acceptance of and willingness to use digital spaces have also dramatically increased. Social media has become a centrepiece of our social and political lives, and the COVID-19 pandemic has strongly contributed to our spending increased time in digital spaces, both for work and leisure. Meta claims that the Metaverse it proposes to create will further blend the physical and digital worlds, seamlessly integrate our physical and sensory experiences with digital ones, increase the immersiveness of social media and our digital experiences, and make these experiences nearly ubiquitous and increasingly real.

If metaverses are to be the next credible evolution of our societal digitalisation, a thorough discussion of their potential drawbacks is both timely and necessary.

However, recent years have demonstrated how the increased prevalence of social media platforms and digitalisation in our societies has not only had positive consequences. Metaverses, as new ubiquitous and immersive social media spaces, could exacerbate many of the already negative tendencies generated by current social media platforms and lead to new issues surrounding digital crime and online extremist radicalisation, while accentuating geopolitical tensions. They could also increasingly decouple digital and physical life, leading to consequential questions about human relations and the legitimacy of traditional socio-political and economic institutions. If metaverses are to be the next credible evolution of our societal digitalisation, a thorough discussion of their potential drawbacks is both timely and necessary. Anticipatory attitudes towards the risks they pose will ensure we do not find ourselves again in our current situation, where some technologies are so ingrained in our societies and economies that it has become extremely difficult to design and implement the measures needed to mitigate their negative impacts. Security-by-design and risk mitigation measures should therefore be key and non-negotiable elements of efforts to develop metaverses.

What is a metaverse? A brief history

The term "metaverse" is largely attributed to US fiction author Neal Stephenson, who first coined it in his 1992 novel *Snow Crash*. No one definition exists for a metaverse, but it can be loosely characterised as an immersive virtual environment that utilises technologies such as augmented reality (AR) and virtual reality (VR) (among others) to seamlessly mesh the physical and virtual worlds. In such an environment, entering and utilising digital spaces would no longer require narrow access points such as computer screens or smartphones. Since its birth in fiction, various attempts at building a metaverse have been made, with varying degrees of success. Online media platform Second Life, which launched in 2003, is perhaps the most notable example of an immersive virtual reality world that pre-dates the age of social media.[3]

The relative maturity of these enabling technologies and our increased comfort with working, socialising, and generally operating in digital spaces fostered by the COVID-19 pandemic are laying the foundations for metaverses to become a reality.

While Facebook is not the first or the only company to be interested in building a metaverse, its rebranding as Meta in late 2021 focused renewed attention on the concept, making it a buzzword, and potentially represents a new turning point in the history of metaverses. In Meta's vision of its planned Metaverse, users would be able to create avatars of themselves and navigate virtual worlds where they could play games, watch movies, have meetings, attend social events or even buy property.[4] The distances that are intrinsic to the physical world will be completely erased in this entirely artificial world, which will have no physical limitations. For their realisation, metaverses such as this will require underlying technologies such as VR and AR, ubiquitous sensors, and blockchain-enabled cryptocurrencies to support their virtual economies so that users can buy and sell digital assets.[5] All this will require enormous computing power and huge amounts of energy.

The relative maturity of these enabling technologies and our increased comfort with working, socialising, and generally operating in digital spaces fostered by the COVID-19 pandemic are laying the foundations for metaverses to become a reality. But it is important to note that while some of its foundational technologies are at various stages of maturity, a metaverse as a unified and perpetual 3D virtual space merged with our physical surroundings does not yet exist. Today, the metaverse is a *vision* of what the next evolution of the Internet could be. As such, one must be cautious about taking the assertions of Big Tech companies as to what the various versions of the metaverse that they propose will actually be like at face value. Those responsible for creating these metaverses – and profiting from selling their services to consumers/users – might well oversell their future capacities.

Potential benefits

Metaverses will further the dematerialisation of the world that started with the Internet, and give people access to more information, experiences, connections and knowledge than ever before. Indeed, metaverses will provide people with access to a wealth of new sensory and dematerialised experiences and connections. This will come with a wide array of new opportunities for individuals, businesses, content creators and artists.[6] Some society-wide beneficial impacts might ensue. For example, the possibility of more immersive digital relationships could lead to ever-more-meaningful relationships with individuals across the globe, more so than what is already possible today.

Additionally, some digital experiences are currently still plagued by limitations, such as the physical discomfort (or even pain) often

associated with spending hours sitting in front of a screen or the difficulty of replicating workspace environments and relationships in remote working contexts. Metaverses promise to make these interactions closer to their real-world equivalents and do away with the friction created by accessing digital experiences through a screen.[7] Yet, although metaverses offer potential benefits, we will also need to discuss their potential negative implications so as to help build a technology that will prevent these possible implications from becoming reality.

Online disinformation and political polarisation

Content bubbles will become increasingly harder to "escape", and disinformation and manipulation will spread faster and become even more efficient as the digital environment in which they exist becomes more immersive and "real".

The most basic and fundamental characteristic of a metaverse is its ubiquity, i.e. its potential to be present in every aspect of our lives and physical environment(s). It follows that companies such as Meta, which are aiming to build and control this new digital/physical space, will become even more present and influential in our everyday lives and interactions than they already are today. Because Facebook's current dominance in some aspects of our lives already comes with serious challenges[8] (addiction, disinformation, social polarisation, etc.), it is to be feared that integrating the company's products and applications into more aspects of our lives will lead to even greater challenges, adding additional layers of complexity — and potential misuse/abuse – to pre-existing problems.

One such challenge is the spread of online disinformation, misinformation, and hate speech that have led to real-world violence, conflict escalation, and political polarisation.[9] Facebook has shown little capacity to successfully stem the spread of disinformation and hate speech; indeed, as internal documents show, the company was fully aware that its services can lead to the above-mentioned problems.[10] A notable example is the company's failure to meaningfully curb election-related disinformation. Notably, Facebook/Meta also disastrously fails to moderate content outside of the United States, which has contributed to its platform being used, for instance, to stoke hate and real-world ethnic violence in Ethiopia and against the Rohingya minority group in Myanmar.[11]

The failure to moderate current information ecosystems in its existing applications shows that Meta is likely to fail in the more complex and connected "application of applications" that will be its Metaverse.[12] The meshing of the physical world with the virtual world by companies like Meta could embed the social media features that enable the spread of disinformation, and thus foster political and social polarisation to an even greater extent in our societies.[13] Because these companies' revenue models focus on the monetisation of data, the maximisation of data generation – often by prioritising polarising content – is a central feature of their business models.[14] By adding a level of immersivity, content bubbles will become increasingly harder to "escape", and disinformation and manipulation will spread faster and become even more efficient as the digital environment in which they exist becomes more immersive and "real". Online gaming, particularly its mechanics, is seemingly offering the blueprints for the construction of metaverses, as exemplified by Microsoft's high-profile purchase of Blizzard Activision – one of the world's largest developers, publishers and distributors of video games – as part of its metaverse creation efforts.[15] Online gaming is already a potent avenue for online disinformation, trolling and the spread of conspiracy theories.[16] Embedding these gaming dynamics in the next iteration of social media might also further embed these

behaviours in more and more areas of our lives, both public and private. Importantly, using gaming dynamics and graphics will greatly facilitate the unquestioned adoption of metaverses by new generations that are already fully immersed in these gaming ecosystems.

Content moderation in a metaverse would be so complex that it would largely be outsourced to algorithms, which have already been shown to have major shortfalls – due to their embedded and learned biases, lack of transparency, and ease of manipulation – when dealing with societally relevant tasks.[17] If people are to spend most of their lives in metaverses, successfully regulating and "policing" the latter's working mechanisms will be foundational to a properly functioning society. It therefore follows that it is becoming increasingly necessary to hold meaningful discussions on how much power societies are willing to delegate to algorithms for managing such vital spaces, and how appropriate and safe these algorithms are at present and will be in the future.[18]

With more data and better profiling capacity, Big Tech's capacity for behavioural manipulation and exercising control over our social and political lives will be exacerbated.

Privacy and personal profiling

The fact that the business models of the companies building metaverses revolve around monetising users' attention has not changed. Specifically, the imperative to better profile individuals to increase the accuracy of advertisement targeting remains Meta's primary aim.[19] Because of this, privacy and issues of data ownership should be central concerns of the development of metaverses.[20] Indeed, metaverses are vehicles that could quantify and "data-ify" information about potential users who had previously escaped social media companies, because these individuals' interactions occurred physically in the real world and not digitally on these companies' platforms.[21] If tech companies are able to use metaverses to move more of our lives and activities online and merge the physical and virtual, they will be able to collect previously untapped behavioural data, because platforms will be able to track body movements and – possibly more importantly – physiological responses to an increased amount of specific stimuli.[22] Metaverse ecosystems will be composed of immersive environments that rely on hardware and sensors capable of increasingly generating new types of data. For instance, some headsets already being used to access fairly basic augmented reality environments are now equipped with sensors that monitor brain activity.[23] Increasingly, haptic devices will allow users to "feel a real environment augmented with synthetic haptic stimuli".[24] Goggles that will be used to access metaverses will similarly be able to track eye movements, providing crucial data about the users' foci of attention and thus their interests and priorities.[25]

These new sensors will be able to generate new types of data that Internet 2.0 is currently unable to generate.[26] This, in turn will lead to ever-more-accurate user profiling and targeting. The increased ubiquity of data collection will mean that the type of data collected will also be more sensitive, putting a renewed focus on data privacy (who controls the data; who has access to it). Literature on surveillance capitalism has already showed the capacity of Big Tech companies to manipulate real-world behaviour in order to maximise profits through the accurate profiling of their products' consumers.[27] With more data and better profiling capacity, Big Tech's capacity for behavioural manipulation and exercising control over our social and political lives will be exacerbated. This could also lead to the further monopolisation of digital spaces, giving private technology corporations more power and knowledge and an ever-greater capacity to control human behaviour.[28]

Personal security, cyber bullying and harassment

Metaverses could also provide more avenues for cyber bullying and online harassment in ways that would be harder for victims to evade.[29] Indeed, some worry that the mimicking of physical social interactions without the "physical" consequences of anti-social or harassment behaviour could lead to the rampant proliferation of such behaviours in virtual spaces.[30] Trials seem to indicate that people do not generally display the same set of social standards in digital environments, where the lack of physicality and relative anonymity can lead them to behave negatively towards others.[31] Most importantly, evidence shows that online sexual harassment and racial discrimination can have the same emotional effects on victims as their real-world equivalents.[32] In a Meta beta test[33] of Horizon Worlds – the company's virtual reality social media platform – a female tester reported having been digitally groped.[34] Other such incidents involving simulated groping and ejaculation have occurred on other VR games such as *Population One*.[35] In these incidents, safeguards to protect the victims were few and inefficient, and the perpetrators were emboldened by a sense of impunity. Our legal system is woefully unprepared for preventing or penalising offences such as these. Because the psychological consequences of abuse are real however it is inflicted (i.e. in the real world or online), what would constitute digital rape or sexual assault? Questions like these must be resolved before virtual spaces become widespread, to avoid impunity for acts of digital harassment and sexual aggression.

Metaverses could also provide more avenues for cyber bullying and online harassment in ways that would be harder for victims to evade.

Moderating such behaviour online is already proving to be difficult for Facebook: even as it currently only means scanning written and video content. In metaverses, moderating users' behaviour would mean processing spoken language, visible gestures and users' body movements. This is humanly and computationally much more difficult and represents even more of a grey area for moderators than on current social media platforms.[36] Additionally, leaked documents and information from Facebook whistle-blower Frances Haugen shows that, even when it was aware of the nefarious consequences of its platform (e.g. social division, body image negativity, disinformation), Facebook was unwilling to take substantial steps to mitigate these consequences because such measures would have negatively impacted its profits. This gives concerned stakeholders reason to believe that Meta's moderation and safety measures might fall short of protecting its users in the Metaverse it intends to design and market. Indeed, it has been reported that internal Meta memos have stated that "moderating what people say and how they act in the Metaverse at any meaningful scale is practically impossible".[37]

Furthermore, there are plenty of unanswered questions about what operating through avatars would humanly and socially entail, because it will affect how people present themselves, perceive their and others' bodies, and interact in virtual spaces.[38] For instance, the body filters already available on current social media platforms are leading to body dysmorphia issues in young and teenage girls, openly promoting a form of virtual "plastic surgery" at very young ages.[39] It is very likely that metaverses will compound such problems and even create new ones.[40] What will the "avatarisation of society" mean? Will we start giving more credence to our digital selves than our physical selves? Will we value our online world and societies more than our physical-world societal systems and their institutions? If people spend most of their time in a virtual immersive environment, how will this impact their real social

relations? And how will it impact the relationship between the state and its citizens? Will people still be bound by the social contract and give credence to the authority of the state? These unanswered questions have consequences for the future of human society as a whole.

Criminality in the metaverse

Metaverses could also impact international security in a more traditional sense. For example, researchers at the University of Nebraska's National Counter-terrorism, Innovation, Technology and Education Centre have raised concerns over metaverses' potential for aiding terrorist groups in their coordination and recruitment campaigns.[41] They maintain that "online recruitment and engagement are hallmarks of modern extremism, and the metaverse threatens to expand this capacity by making it easier for people to meet up".[42] While the process of radicalisation is complex and the importance and extent of its online element are still disputed, the Internet seems to facilitate the process at least through the ease with which information can be disseminated, the amplification of group polarisation, and the legitimisation of extreme ideology and violence through online echo chambers.[43] However, offline "push factors" and interactions still play an important role in the radicalisation process.[44] Metaverses could become a powerful tool for extremist groups to expand their ranks by intensifying the aspects of the Internet that facilitate radicalisation and through the possibility of enabling more realistic personal "virtual" relationships that would reduce the importance of the "offline" element of radicalisation. Furthermore, one could posit that metaverses could make it easier for terrorist groups to conduct reconnaissance and coordinate attacks, notably by digitally replicating targets and rehearsing attacks beforehand.[45]

Metaverses by "connecting many technologies, which increase data sharing like never before", will massively expand the attack surface and, thus, the potential vulnerabilities in cyber security.

Online games are a common vector and target for paedophiles and other sexual predators.[46] If the more realistic replication of real-world interactions is coupled with the ease of meeting in virtual spaces, child grooming and the establishment of predatory relationships could happen easier and quicker.[47] Facebook's relative failure to enforce robust user integrity (e.g. by spotting and closing down fake accounts) raises questions over the ease with which predators will be able to create fake accounts and use non-threatening avatars to hide their true motives in the proposed Metaverse.[48]

In general, metaverses additionally offer novel avenues for economic crime, theft and scams. On Sandbox, self-described as a "virtual metaverse where players can build, own and monetize their virtual experiences", scammers are already stealing and selling others' virtual property.[49] The increased digitalisation of assets multiplies their vulnerability to cyber attacks and other forms of fraudulent activity.[50] For example, it is possible to steal someone's land or digital home in a metaverse. If people are to spend an increasing amount of their time (and money) in the digital spaces they own, the effects of property theft would be similar to those of its real-world equivalent. The patchy – and sometimes non-existent – regulation of crypto currencies and NFTs[51] not only means that illicit activities such as money laundering are facilitated, but also that there is often little recourse against crime.[52] Overall, metaverses by "connecting many technologies, which increase data sharing like never before", will massively expand the attack surface and, thus, the potential vulnerabilities in cyber security.[53]

The geopolitics of the metaverse

It is impossible to disentangle tech giants from geopolitics, largely because they are at the centre of the technological rivalry between China and the United States.[54] Because the creation of metaverses is supported by the technological juggernauts of both countries, these virtual worlds will play a key role in – and likely heighten – technological tensions between Beijing and Washington. While the jury is still out on whether they will act as an enabler of China-US decoupling or increased interdependence, current developments in the relationship between the two great powers would suggest the former is more likely.[55] Indeed, according to the Eurasia Group, the geopolitics of the metaverse are "likely to mirror trends in the physical world that are pushing towards bifurcation into Chinese and Western-centric technology stacks and data and financial layers".[56] This leads to questions of whether there will be a "western" metaverse controlled by US tech giants and an authoritarian, censored one run by China (and possibly Russia). [57] If this is the case, questions over their interoperability, as well as over the role of other actors such as Europe similarly arise. The borderless vision of metaverses will also likely clash with largely national legal systems and frameworks. This, in turn, could also lead to a backlash favouring technological decoupling.

If the uses of metaverses are to rival those of the Internet, they will become strategic and critical forms of infrastructure and therefore become de facto power-projection instruments used by both state and non-state actors for geopolitical ends.

Technology giants have become economic mammoths, with revenues and market valuations rivalling, and often surpassing, the gross domestic products of states. As we have seen, the reach and ubiquity of their products also make it difficult to isolate them from politics, and they have become part of the global power equation.[58] Social media platforms are, for example, increasingly at the centre of our political lives. This has led to a situation where they are called on to an ever-greater extent to be "social actors" asked to perform "social tasks" such as fighting the spread of disinformation or policing hate speech online. As metaverses grow and the services and products of the companies that design and operate them encompass more aspects of our lives, their importance vis-à-vis our society, politics and economics will grow in tandem. Governments are already finding it hard to take meaningful actions to hold tech giants such as Facebook or TikTok accountable. Governments' capacity to curtail the power of these private entities might only decrease as metaverses grow and people increasingly merge their real with their digital lives. For now, however, with various tech giants vying to build a metaverse, the landscape more realistically resembles multiple proprietary, non-interoperable metaverses owned by Microsoft, Google, Meta, Tencent, Baidu or Alibaba, as opposed to one "single metaverse" operated by one company that has risen above the rest.[59]

Metaverses could also influence future power politics and warfare. In fact, if the uses of metaverses are to rival those of the Internet, they will become strategic and critical forms of infrastructure and therefore become de facto power-projection instruments used by both state and non-state actors for geopolitical ends. Should metaverses come to complement – or even replace – reality, the actors controlling the underlying infrastructure would be able to alter that reality and therefore influence their users' behaviours. As previously described, disinformation will become more powerful in a metaverse; concerted, state-run disinformation campaigns and propaganda would therefore also become more powerful. States could therefore utilise metaverses to manipulate behaviours and alter users' norms to their (i.e. states') advantage. States with limited geopolitical influence in the past have found technological niches to exert greater influence. Turkey, for example, uses the sale and

use of drones to make up for its limited power-projection capabilities.[60] The building, use, control, and weaponisation of metaverses could similarly become a way for some state and non-state actors to develop new tools to exercise influence and enforce coercion, and reinforce the growing influence of surrogates in warfare and the projection of violence.[61] Similarly, the immersiveness of metaverses will also contribute to giving neurotechnologies an ever-increasing role in warfare.[62]

What's next? Neurotechnologies in the metaverse

Metaverses could similarly become a way for some state and non-state actors to develop new tools to exercise influence and enforce coercion, and reinforce the growing influence of surrogates in warfare and the projection of violence.

Recent technological developments in the field of neuroscience and neurotechnologies are rapidly advancing our understanding of the brain and its processes, and enabling the development of increasingly advanced neurotechnologies. These technologies are providing unprecedented capability to read from and write into the brain, enabling the control of robotic prosthetics and computers through the power of thought with the help of brain-computer interfaces.[63] However, the development of neurotechnologies is fraught with ethical, moral, social, political and security risks. For example, from the capability to understand and decode neural processes it is only a short leap to the capability to alter mental states, potentially enabling manipulation for malicious purposes or in corporate and government interests.[64] Because we now increasingly have access to sensitive and private cognitive processes that are at the centre of an individual's personality, behaviour and personhood, key data privacy issues arise, namely who has access to this data and what can be done with it?[65]

While today these technologies are still in their infancy and often require invasive methods, research is rapidly advancing, and more and more private technology firms, such as Elon Musk's Neuralink, are entering the field. It will not be long before neurotechnologies converge with metaverses.[66] In fact, at their current stage of maturity, VR headsets are not the most efficient way of accessing virtual spaces. Their bulkiness and relative awkwardness notwithstanding, it is common among users of such headsets to experience nausea, motion sickness and other symptoms of discomfort after an extended period of using them.[67] This limits metaverses, because it prevents people from wearing VR headsets for extended periods. In time, neurotechnologies could do away with these limitations by enabling people to navigate digital spaces with just the power of their minds. They therefore represent a logical avenue of development for those attempting to design and implement metaverses.

However, the convergence of neurotechnologies with metaverses risks exacerbating some of the challenges referred to above. As previously mentioned, metaverses will serve as a new avenue to feed a business model based on the monetisation of users' attention and behavioural data, because it will enable the collection of previously untapped data. A direct gateway into the minds of consumers represents the next frontier of this business logic. The better profiling capabilities this would enable would result in significantly increased revenues for metaverse companies. Left unregulated, this will not only aggravate issues of privacy and corporate data collection, but risks opening up a new realm of possibilities for manipulation and behavioural influence. Neurotechnologies combined with metaverses could therefore offer new tools for coercion and the exercising of such influence.[68] The cognitive dimension of warfare, which seeks to change how members of a target group think and, as a result, how they act will therefore be reinforced.

Ultimately, metaverses could substantially contribute to cognitive warfare aimed at leveraging, disrupting or influencing basic belief structures in adversaries (both civilian and military) in ways that digitally influence their physical behaviours.[69]

Where do we go from here?

A good starting point for discussions on the future metaverse or metaverses is to look back and learn from the past. The current backlash against Big Tech is the result of decades of technological innovation divorced from concerns over potential negative impacts. This is largely due to the naive optimism that surrounded the birth of the Internet, which was imagined as a liberating technology that would provide knowledge to everybody on the planet and spread liberal values worldwide.[70] Looking forward armed with our knowledge of what has actually happened in this regard, it is imperative to take a different approach to technological development – one that considers both the advantages and disadvantages of the process, and does not rely on the highly questionable principle of developing and deploying technology as quickly as possible and dealing with the problems later. Security-by-design and responsible innovation should be the chief guiding principles of the development of metaverses. In today's environment of political polarisation and disinformation powered by social media, Facebook's old "move fast and break things" motto is particularly disturbing. Because the metaverse currently still remains on the horizon, now is the perfect time to think about its potential drawbacks and misuses. This will enable the creation of the necessary guardrails to ensure that metaverse technology is developed and deployed in ways that address and minimise its potential risks in a meaningful way.

Ultimately, metaverses could substantially contribute to cognitive warfare aimed at leveraging, disrupting or influencing basic belief structures in adversaries (both civilian and military) in ways that digitally influence their physical behaviours.

Endnotes

1. This Strategic Security Analysis intentionally uses different ways of spelling and using the word "metaverse". The expression "the metaverse" refers to the concept in general, whereas "the Metaverse" with a capital *m* refers to Meta's (formerly Facebook's) proposed product. When referring to "a metaverse", we are referring to a hypothetical, non-specific metaverse; the same applies to "metaverses".

2. Meta has reportedly invested US$10 billion in its Metaverse project. Other such projects include those of Microsoft, Nvidia, Tencent and videogame company Roblox.

3. R. Lawler, "Second Life Joins the Metaverse Discussion with the Return of Its Founder – and Some Key Patents", *The Verge*, 13 January 2022, https://www.theverge.com/2022/1/13/22881864/metaverse-second-life-decentralized-moderation-patent-virtual-reality.

4. O. Carmiel, "Virtual Land Prices Are Booming, and Now There's a Fund for That", Bloomberg, 19 March 2021, <https://www.bloomberg.com/news/articles/2021-03-19/virtual-land-prices-are-booming-and-now-there-s-a-fund-for-that>.

5. A. Robertson and J. Peters, "What Is the Metaverse, and Do I Have to Care?", *The Verge*, 4 October 2021, https://www.theverge.com/22701104/metaverse-explained-fortnite-roblox-facebook-horizon.

6. A. Takyar, "Metaverse Use Cases and Benefits", LeewayHertz, n.d., https://www.leewayhertz.com/metaverse-use-cases-and-benefits/#:~:text=A%20platform%20based%20on%20Metaverse,present%20social%20media%20universe's%20abilities.

7. C. Newton, "Mark in the Metaverse", *The Verge*, 22 July 2021, https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview.

8. MIT Initiative on the Digital Economy, *Social Media at a Crossroads: 25 Solutions from the Social Media Summit @ MIT*, 2021, https://ide.mit.edu/wp-content/uploads/2021/10/The-SMS@MIT-Report.pdf?x57209.

9. K. Hao, "How Facebook and Google Fund Global Misinformation", *MIT Technology Review*, 20 November 2021, https://www.technologyreview.com/2021/11/20/1039076/facebook-google-disinformation-clickbait/.

10. J. Deutsch et al., "Misinformation Has Already Made Its Way to the Metaverse", Bloomberg, 15 December 2021, https://www.bloomberg.com/news/articles/2021-12-15/misinformation-has-already-made-its-way-to-facebook-s-metaverse.

11. Hao, 2021.

12. S. Ghaffary, "Why You Should Care about Facebook's Big Push into the Metaverse", *Vox*, 24 November 2021, https://www.vox.com/recode/22799665/facebook-metaverse-meta-zuckerberg-oculus-vr-ar.

13. J.-M. Rickli and A. Kaspersen, "The Global War of Narratives and the Role of Social Media", *World Economic Forum*, 8 July 2016, https://www.weforum.org/agenda/2016/07/the-global-war-of-narratives-and-the-role-of-social-media/.

14. D. Lauer, "Facebook's Ethical Failures Are Not Accidental; They Are Part of the Business Model", *AI and Ethics*, Vol.1, May 2021, pp.395-403, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8179701/pdf/43681_2021_Article_68.pdf.

15. K. Weise et al., "Microsoft Will Buy Activision Blizzard, Betting $70 Billion on the Future of Games", *New York Times*, 18 January 2022, https://www.nytimes.com/2022/01/18/business/microsoft-activision-blizzard.html.

16. Z. Weinberg, "The Metaverse Is Coming, and the World Is Not Ready for It", *New York Times*, 2 December 2021, https://www.nytimes.com/2021/12/02/opinion/metaverse-politics-disinformation-society.html.

17. R. Di Pietro and S. Cresci, "Metaverse: Security and Privacy Issues", Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, 2021, https://www.researchgate.net/publication/357116743_Metaverse_Security_and_Privacy_Issues.

18. Ibid.

19. S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London, Profile Books, 2019, pp.8-9.

20. Di Pietro and Cresci, 2021.

21. I. Bogost, "The Metaverse Is Bad: It Is Not a World in a Headset but a Fantasy of Power", *The Atlantic*, 21 October 2021, https://www.theatlantic.com/technology/archive/2021/10/facebook-metaverse-name-change/620449/.

22. Di Pietro and Cresci, 2021.

23. A. Robertson, "MindMaze's Hand-tracking, Mind-reading Virtual Reality Headset Is Just as Complicated as It Sounds", *The Verge*, 4 March 2019, https://www.theverge.com/2015/3/3/8136405/mind-maze-mind-leap-thought-reading-virtual-reality-headset.

24. J. Seokhee and S. Choi, "Haptic Augmented Reality: Taxonomy and an Example of Stiffness Modulation", *IEEE Xplore*, 1 October 2009, https://ieeexplore.ieee.org/document/6797520.

25. I.A. Hamilton, "Meta Wants to Track Your Eye Movements and Facial Expressions as You Roam the Metaverse, Patents Suggest", *Business Insider*, 18 January 2022, https://www.businessinsider.com/meta-metaverse-patents-track-eye-movement-facial-expressions-facebook-zuckerberg-2022-1?r=US&IR=T.

26. Internet 2.0 or Web 2.0 refers to "The second stage of development of the internet, characterized especially by the change from static web pages to dynamic or user-generated content and the growth of social media."; https://www.lexico.com/definition/web_2.0 , see also J. Drake, "How We Can Finally Evolve from Web2 to Web3," *VentureBeat*, 13 February 2022, https://venturebeat.com/2022/02/13/how-we-can-finally-evolve-from-web-2-0-to-web-3-0/.

27. Zuboff, 2019, pp.202-203.

28. D. Stolle, "We Need to Kick Big Tech out of the Metaverse", *Wired*, 7 July 2021, https://www.wired.co.uk/article/metaverse-big-tech.

29. S. Frenkel and K. Browning, "The Metaverse's Dark Side: Here Come Harassment and Assaults", *New York Times*, 30 December 2021, https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html; P. Olson, "Its Awkward Being a Woman in the Metaverse", Bloomberg, 15 December 2021, https://www.bloomberg.com/opinion/articles/2021-12-15/the-metaverse-via-oculus-is-awkward-if-you-re-a-woman-and-beware-of-griefers?sref=5MgY8FTh.

30. Olson, 2021; Deutsch et al., 2021.

31. T. Basu, "The Metaverse Has a Groping Problem Already", *MIT Technology Review*, 16 December 2021, https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/.

32. Ibid.

33. "Beta testing is an opportunity for real users to use a product in a production environment to uncover any bugs or issues before a general release"; ProductPlan, "Beta Test", 2022, https://www.productplan.com/glossary/beta-test/.

34. Basu, 2021.

35. Frenkel and Browning, 2021.

36. Olson, 2021.

37. Frenkel and Browning, 2021.

38. Basu, 2021.

39. T. Ryan-Mosely, "Beauty Filters Are Changing the Way Young Girls See Themselves", *MIT Technology Review*, 2 April 2021, https://www.

technologyreview.com/2021/04/02/1021635/beauty-filters-young-girls-augmented-reality-social-media/.

40. Basu, 2021.

41. J.S. Elson et al., "The Metaverse Offers Much Potential for Terrorists and Extremists", Defence One, 10 January 2022, https://www.defenseone.com/ideas/2022/01/metaverse-offers-much-potential-terrorists-and-extremists/360503/.

42. Ibid.

43. G.N. Molmen and J.A. Ravndal, "Mechanisms of Online Radicalisation: How the Internet Affects the Radicalisation of Extreme-right Lone Actor Terrorists", *Behavioral Sciences of Terrorism and Political Aggression*, 30 October 2021, https://www.tandfonline.com/doi/pdf/10.1080/19434472.2021.1993302.

44. Ibid.

45. Elson et al., 2022.

46. N. Bowles and M.H. Keller, "Video Games and Online Chats Are 'Hunting Grounds' for Sexual Predators", *New York Times*, 7 December 2019, https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html.

47. T. Lloyd, "Facebook's Metaverse Heralds a Brave New Underworld of Metacrime", *New Republic*, 29 November 2021, https://newrepublic.com/article/164497/facebook-metaverse-cybercrime-marc-zuckerberg.

48. Ibid.

49. L. White, "Sandbox Metaverse Hackers Are Stealing Virtual Property Worth Tens of Thousands of Dollars", Stealthoptional, 11 January 2022, https://stealthoptional.com/news/sandbox-metaverse-hackers-stealing-virtual-property/.

50. K. Alspach, "Why the Fate of the Metaverse Could Hang on Its Security", VentureBeat, 26 January 2022, https://venturebeat.com/2022/01/26/why-the-fate-of-the-metaverse-could-hang-on-its-security/.

51. Non-fungible tokens.

52. T. Wilson, "Crypto Crime Hit Record $14 Billion in 2021, Research Shows", Reuters, 6 January 2022, https://www.reuters.com/markets/us/crypto-crime-hit-record-14-billion-2021-research-shows-2022-01-06/; Lloyd, 2021.

53. SocRadar, "Future of Cybersecurity in the Era of the Metaverse", 4 March 2022, https://socradar.io/future-of-cybersecurity-in-the-era-of-metaverse/.

54. R. Hass et al., "U.S.-China Technology Competition: A Brookings Global China Interview", Brookings, 23 December 2021, https://www.brookings.edu/essay/u-s-china-technology-competition/.

55. Ibid.

56. Eurasia Group, "The Geopolitics of the Metaverse: No Escaping Bifurcation", December 2021, p.2, https://www.eurasiagroup.net/files/upload/EurasiaGroup_TheGeopoliticsOfTheMetaverse.pdf.

57. Ibid.

58. O. Jonnson, *How Do You Invade Facebook?*, Swedish Entrepreneurship Forum, 2022, https://entreprenorskapsforum.se/wp-content/uploads/2022/03/Rapport_Jonsson_web.pdf.

59. C. D'Anastasio, "The Metaverse Is Simply Big Tech, but Bigger", *Wired*, 4 November 2021, https://www.wired.com/story/big-tech-metaverse-internet-consolidation-business/.

60. L. Hofman, "How Turkey Became a Drone Power (and What That Tells Us about the Future of Warfare)", *The Correspondent*, 10 December 2019, https://thecorrespondent.com/832/how-turkey-became-a-drone-power-and-what-that-tells-us-about-the-future-of-warfare.

61. A. Krieg and J.-M. Rickli, *Surrogate Warfare: The Transformation of War in the Twenty-first Century*, Georgetown, Georgetown University Press, 2019, http://press.georgetown.edu/book/georgetown/surrogate-warfare.

62. J.-M. Rickli, "Neurotechnologies and Future Warfares", RSIS Commentary, RSIS, Nanyang Technological University, 7 December 2020, https://www.rsis.edu.sg/rsis-publication/rsis/ai-governance-and-military-affairs-neurotechnologies-and-future-warfare/#.YAp-Oi2ZPEZ.

63. S. Saha et al., "Progress in Brain Computer Interface: Challenges and Opportunities", *Frontiers in Systems Neuroscience*, 25 February 2021, https://www.frontiersin.org/articles/10.3389/fnsys.2021.578875/full#B241.

64. E. Strickland, "Worldwide Campaign for Neurorights Notches Its First Win", *IEEE Spectrum*, 18 December 2021, https://spectrum.ieee.org/neurotech-neurorights.

65. M. Ienca, "We Must Expand Human Rights to Cover Neurotechnology", ETH Zurich, 7 October 2021, https://ethz.ch/en/news-and-events/eth-news/news/2021/10/marcello-ienca-we-must-expand-human-rights-to-cover-neurotechnology.html.

66. C. Hackl, "Now Is the Time to Talk about Ethics and Privacy in the Metaverse", *Forbes*, 2 August 2020, https://www.forbes.com/sites/cathyhackl/2020/08/02/now-is-the-time-to-talk-about-ethics--privacy-in-the-metaverse/?sh=45a4a8c1ae6c.

67. W. Gordon, "How to Reduce Motion Sickness in Virtual Reality", *Wired*, 22 April 2021, https://www.wired.com/story/how-to-reduce-motion-sickness-virtual-reality/.

68. J.-M. Rickli and M. Ienca. "The Security and Military Implications of Neurotechnology and Artificial Intelligence", in O. Friedrich et al. (eds), *Clinical Neurotechnology Meets Artificial Intelligence: Philosophical, Ethical, Legal and Social Implications*, Berlin, Springer, 2021, pp.197-214, https://link.springer.com/chapter/10.1007/978-3-030-64590-8_15.

69. F. du Cluzel, *Cognitive Warfare*, NATO Innovation Hub, 2020, https://www.innovationhub-act.org/sites/default/files/2021-01/20210113_CW%20Final%20v2%20.pdf.

70. D. Weinberger, "The Internet That Was (and Still Could Be)", *The Atlantic*, 12 June 2015, https://www.theatlantic.com/technology/archive/2015/06/medium-is-the-message-paradise-paved-internet-architecture/396227/.

GCSP
Geneva Centre for Security Policy

Where knowledge meets experience

The GCSP Strategic Security Analysis series are short papers that address a current security issue. They provide background information about the theme, identify the main issues and challenges, and propose policy recommendations.

Geneva Centre for Security Policy - GCSP
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
CH - 1211 Geneva 1
Tel: + 41 22 730 96 00
Fax: + 41 22 730 96 49
e-mail: info@gcsp.ch
www.gcsp.ch

ISBN: 978-2-88947-310-6