WORLD ECONOMIC FORUM

Metaverse Cybersecurity: Building Resilience in the Future Internet

BRIEFING PAPER

JUNE 2024

Images: Getty Images

Contents

Foreword 3

Introduction 4

1 Unlocking value and mitigating risk 5

1.1 Privacy 5

1.2 Virtual assets 7

1.3 Safety 7

1.4 Political systems 9

Conclusion 10

Contributors 11

Endnotes 17

Foreword

Daniel Dobrygowski
Head of Governance and Trust
World Economic Forum

The ongoing history of the internet can be described as a series of innovative disruptions, continuously shifting the habits of consumers, industries, regulators and observers alike. Since its broader release to the public in 1993, the World Wide Web has facilitated the advent of novel innovations such as social media and online payment systems, resulting in profound departures from traditional means of information sharing, human interaction and commerce. These, and other, innovations have catalysed many new avenues for global economic opportunity and improved communication.

Yet, innovation is not without risk. In addition to the opportunities developed throughout internet ecosystems, there are ever-evolving pathways for harm and exploitation rooted in systemic and user vulnerabilities, often inadvertently aided by lagging or ineffective governance mechanisms. To build trust in current and future iterations of the internet, care must be taken to safeguard users, minimize and mitigate harms, and increase the availability of beneficial opportunities.

The governance track of the World Economic Forum's Defining and Building the Metaverse Initiative is pleased to contribute to this global conversation on the governance principles needed to foster responsible and ethical cybersecurity mechanisms for a resilient, safe and trustworthy future internet.

Introduction

The integration of augmented reality (AR), virtual reality (VR) and extended reality (XR) throughout centralized and decentralized platforms is facilitating immersive experiences that offer boundless consumer and industry value across multiple sectors. As these frontiers continue to offer enhanced communication and connectivity, the future of the internet presents new avenues for global interaction and innovation. Therefore, ensuring resilient digital ecosystems that support secure environments for diverse global usership is imperative to realizing the potential of the metaverse and its place as one of the drivers for the internet's unfolding future.

Protecting the next phase of the internet requires a preventative, forward-looking approach that involves the whole of society and prioritizes building trust, promoting agency and safeguarding user experiences. While systems are not impenetrable and platforms are not impervious, stakeholders can mitigate long-term risk by approaching cybersecurity through a focus on resilience, the ability for systems to operate under attack and recover efficiently.[1]

As part of the ongoing work of the governance track of the World Economic Forum's Defining and Building the Metaverse Initiative, this briefing paper outlines the unique cybersecurity challenges associated with the metaverse and the next phase of the internet. It seeks to guide the attention of decision-makers and developers with the ethical, resilient cybersecurity considerations from a global governance perspective, with the purpose of tackling these cyber risks while they are still in their nascent stages – to prepare metaverse ecosystems to stand against harms posed by threat actors and sustain through undesired behaviours by users or systems themselves.

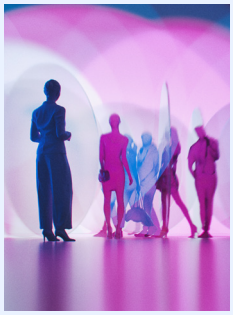
1 Unlocking value and mitigating risk

The next phase of the internet offers a paradigm shift for social and economic value creation predicated upon immersive experiences and further integration of financial infrastructure,[2] spanning multiple jurisdictions.

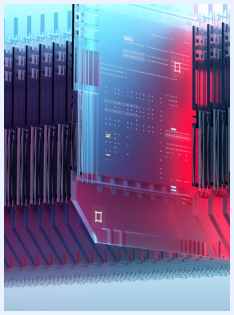
These developments, without proper governance measures, may produce a set of unmitigated security risks, targeting different facets of user safety and experiences that can be evaluated through four thematic areas.

Privacy

Virtual assets



Safety



Political systems

Evaluation of threats to immersive environments through these four thematic camps allows for pragmatic and action-oriented governance recommendations that are, reliable, lasting and sustainable. These recommendations support the security dimension of the World Economic Forum's Digital Trust Framework to ensure metaverse technologies are being deployed to "protect all stakeholders' interests and uphold societal expectations and values."[3]

1.1 Privacy

Risks to data and identity

The metaverse is widening the user's data exhaust – the trail of data generated by a system from a user's activity, behaviour and transactions. In addition to all forms of data previously generated by internet use and online activity, metaverse technologies broadly expand the landscape of generated data types, potentially exposing users to more frequent, varied and consequential security risks due to data breaches, identity theft and surveillance.

Data breaches

Cyberattacks resulting in data breaches compromise invaluable information such as institutional financial records, sensitive employee information and privileged client data. This can result in the suspension of operations, significant financial loss and severe reputational damage. High-profile cases of data breaches in recent years involving the targeting of US government agencies through contractors[4] highlight the severity of such an attack on metaverse platforms, especially as nation-states have begun building metaverse ecosystems to train government employees or provide remote services to citizens and stakeholders.[5]

Identity theft

The most likely outcome of a data breach on an individual level is identity theft.[6] In metaverse ecosystems, identity theft can have far-reaching consequences, including impersonation and fraud, loss of credentials, and access to virtual assets or accounts.

The theft of metaverse credentials can be used to access stored personal information, including highly valuable and non-duplicative forms of data such as iris scans or fingerprints. These can then be sold for profit to nefarious actors who may use the data to commit crimes in both virtual and physical settings.

In large corporate settings, compromising the metaverse identity or credentials of only a single employee can endanger entire organizations.

A unique identity-related risk in the metaverse pertains to the creation and storage of avatar data. As the representation of digital identity in immersive spaces, avatars[7] are a means of access to communal virtual spaces. The theft of an avatar can therefore be understood as the theft of digital identity, and this may lead to impersonations and enable a threat actor to engender unearned trust, access private spaces and communications, defame the impersonated user, hijack their likeness to spread disinformation, and conduct harassing or abusive behaviours with impunity.[8]

The personal and reputational impact of all these harms is amplified by the visceral connection the metaverse provides users to their digital environments and the peers they engage with via avatars within those spaces.

Identification and surveillance

The metaverse requires access points for users to enter immersive, simulative, or layered reality experiences that will rely on the physical body to control virtual and digital activity. That digital activity leaves a more tangible and pervasive trail linking digital behaviour to a physical user. A UC Berkeley study found that when a machine learning algorithm was trained on public use data of head and hand motion from a rhythm-based VR game, the algorithm was able to identify users from a pool of 50,000 with 94% accuracy using only 100 seconds of use data.[9]

> Without responsible data stewardship, user data could be subject to undue monitoring, manipulation, monetization and surveillance.

While data is a net-neutral byproduct of engagement in immersive technology, it is difficult to understand the extent to which bodily data is being collected, stored and processed. Without responsible data stewardship, user data could be subject to undue monitoring, manipulation, monetization and surveillance.

Governance outlook

Protecting metaverse privacy requires modernizing data conceptions and stewardship practices to account for new and more voluminous data collection and risk vectors associated with XR technologies.

There are many avenues to progress this modernization, including, but not limited, to:

- Augmenting consent protocols to ensure users fundamentally understand the breadth of data collection and use to which they are agreeing.
- Robustly categorizing captured data and attributing rigorous standards to net-new data types, such as treating body-based use data as health data.
- Developing multi-factor authentication and account compromise detection protocols consistent with the state of metaverse technologies.
- Developing ethical industry standards for third-party data and information sharing across jurisdictions.

1.2 Virtual assets

$20 billion

Tissuntiat porum hit aut reped quas dolores sequuntiatis vendae ne pere litatium con.

Digital assets are broadly defined by the Financial Action Task Force (FATF) as "any digital representation of value that can be digitally traded, transferred or used for payment".[10] This can include cryptocurrencies such as bitcoin, non-fungible tokens (NFTs), and gaming tokens available to consumers in Web3 and immersive spaces. While gaming tokens may be valuable only within virtual localities, cryptocurrencies and NFTs may present tangible value more broadly. Bitcoin, for example, reached an all-time high value exceeding $70,000 in early March of 2024[11] and NFTs can link ownership of assets between the physical and digital worlds.[12] In the past, tokens and virtual currencies were only valuable within the confines of a host platform, but as an interoperable, metaverse-driven internet develops, virtual currencies and assets are foundational to building and deriving value in blended reality.

Security risks of blockchain

Most of the trading of digital currencies is conducted on blockchains,[13] which will continue to propel peer-to-peer transactions and promote transparency and seamless record-keeping. As users navigate Web3, blockchain is poised to be the natural means to facilitate transactional interoperability and the safe transfer of assets, including virtual currencies and virtual goods. It is important to note that blockchain integration is not, by itself, a comprehensive security measure. Blockchain processes can be hacked, leading to significant loss of value.

Theft and fraud

Through social engineering tactics and phishing scams, hackers may gain access to a user's digital wallet and then steal stored digital currency and other virtual assets. It may be difficult to provide adequate redress to victims of theft in the metaverse, particularly if the virtual asset stolen is stored within the confinements of a different legal jurisdiction, with incompatible regulation to that of the victim's point of origin.

Illicit financing

The potential misuse of NFTs includes money laundering, market manipulation, tax evasion, intellectual property crime, terrorist financing and other illicit financial activities. Due to fragmented jurisdictions, virtual assets offer terrorist and criminal organizations a means to leverage inconsistent tracing and governance coupled with the anonymity often associated with virtual assets to launder money or finance illicit activities. In this sense, weak and fragmented governance becomes a cybersecurity vulnerability itself.

Governance outlook

The continued progress of Web3 and XR technologies stands to create transformative commercial value through both net-new digital assets and seamless integration of physical/digital value transfer. To deliver and sustain this value, robust and resilient system protections, networks for information sharing and redress mechanisms must be in place.

Some potential avenues to advancing such protections are:

- Modernize legal definitions and redress channels to account for virtual assets, enabling relevant public sector escalation, enforcement, and support in cases of theft, fraud, etc.
- Standardize basic authentication protocols to access digital wallets.
- Ensure developers are conscientious of foundational privacy, safety and security principles when designing network infrastructure.
- Establish cross-border and jurisdictional information-sharing mechanisms to adequately identify, trace and prosecute metaverse financial crimes.

1.3 Safety

As immersive technologies and digital asset integration bolster the relevance and impact of digital experiences in users' lives, safety in immersive spaces will increasingly impact safety in the physical world. The World Economic Forum's Typology of Online Harms, rooted in human rights principles, "harmonizes universal perceptions of online threats".[1] These harms, which are often not criminalized, must be encoded, and adopted by the international community to ensure adequate recourse and safety standards, with special attention to the needs of vulnerable populations engaging with metaverse technologies, such as children and adolescents.

Child and adolescent safety

Online dangers to children such as cyberbullying, sexual exploitation, grooming, harassment and coercion are well documented within Web2 spaces, and extensive research has been conducted on the psychological ramifications of children's exposure to harmful online content. However, the extent to which experiencing harm in immersive environments may impact children's mental and emotional health or their development remains unknown.

Sexual offenses in the metaverse, targeting users' avatars cause "significant psychological and emotional trauma"[1] and have already occurred in immersive environments.[20] These risks are further compounded by the risk of "phantom touch – brain sensory input that causes the body to experience sensations similar to physical touch"[21]; meaning, victims of sexual assault in virtual reality could experience unwanted physical contact, specifically when using a haptic suit.

Children and their devices must be safeguarded from predators seeking to take advantage of gaps in security measures. Child spaces in metaverse environments must have strong security protocols to ensure unauthorized users cannot access these communities, and age-based controls and adequate reporting mechanisms should be made available to children and parents.

Cybersecurity and physical safety

Emotionally vulnerable users are particularly at risk of falling victim to social engineering tactics being expertly deployed in simulative and layered reality environments. Each year, thousands of people are lured to travel by criminals promising employment or other benefits and are then trafficked and forced to work on scam farms[22] Vulnerable people, such as children, may inadvertently reveal sensitive data about themselves and their families, such as location, preferences, routines and financial information, that could be leveraged by nefarious actors for a myriad of illicit purposes including fraud, money laundering, identity theft and targeted physical violence.

Experiencing immersive or augmented environments safely requires cybersecurity measures that ensure endpoints are not compromised by nefarious actors with malicious intent. Hardware, such as headsets, haptic suits and glasses, can be hijacked[23] leaving users vulnerable to manipulation and interference. Should a hacker gain access to a headset, for example, they could manipulate and distort the user's environment and lead them to inadvertently harm themselves or others. This raises significant concerns surrounding national security, as threat actors could launch an attack that exploits weaknesses in VR/AR/XR hardware and software systems such as "man in the room" attacks[24] to spread malware and other forms of disruptive viruses.

Violence and radicalization

The threat of radicalization is only exacerbated in immersive environments where groups such as terrorist organizations can weaponize the effects of presence and embodiment.[25] These tactics have had historical success as exemplified by the hundreds of thousands of former terrorist fighters and their families remaining in camps across Syria and Iraq following the fall of Da'esh[26] who were either radicalized or scammed online into joining ISIL.

Digital twins

As industrial metaverse use cases advance, the data types available to hackers and scammers will only be widened. Data and information on critical infrastructure vis-à-vis digital twins, as adopted by cities globally to facilitate urban planning and smart development,[27] may incentivize terrorist groups and criminal enterprises to exploit live data of vulnerable targets and assets in metaverse spaces to produce physical harm.

Governance outlook

The critical importance of online safety efforts is well-known, and it will be essential to continue scaling these efforts to meet emerging technological capabilities and risks. Further, it will be essential to supplement safety-by-design with resilience-minded governance efforts aimed at protecting users and systems even after malicious attempts are made.

Examples of resilience-minded efforts include the need to:

- Adopt common conceptions for online harms to enable aligned, cooperative detection and remediation of critical safety threats as and after they appear.
- Develop industry standards for trust and safety, including robust digital literacy and reporting channels with explicit support and response resources dedicated to harms impacting disproportionately vulnerable user groups.
- Apply heightened security standards for stored data pertaining to real-world infrastructure and personally identifiable user information.

"The threat of radicalization is only exacerbated in immersive environments where groups such as terrorist organizations can weaponize the effects of presence and embodiment.

1.4 Political systems

In a report entitled *The Geopolitics of the Metaverse*, the Eurasia Group reports that "incipient metaverses are already breaking down along geopolitical lines".[28] The upshot of this fragmentation is inconsistent regulation and enforcement, leaving greater vulnerability for metaverse exploitation by threat actors. The connection between new avenues of attack and increased incidence of attack is notable; Arkose Labs' 2022 State of Fraud & Account Security report found that metaverse companies experienced 80% more bot attacks and 40% more human attacks than other businesses, as well as being more frequent targets for "master fraudsters".[29]

Fragmented policy

Taking stock of cyberthreats against the metaverse, it becomes increasingly clear that a resilient metaverse will be one that serves a globally distributed consumer and creator base, unbound by the limitations of national borders, supported by global governance and underpinned by interoperability standards. A secure metaverse will not be one developed in a fragmented manner that leaves the future of the internet to be determined by national interest.

Notably, data governance is already differentiating vastly across the European Union, the United States and Chinese jurisdictions,[30] which leads to fragmented data management and inconsistent cybersecurity requirements that make systems susceptible to exploitation. Harmonization across jurisdictions is important to establish minimal cybersecurity and data governance requirements that will prevent governance weaknesses from becoming cybersecurity vulnerabilities themselves. Metaverse hardware and systems must be interoperable so there is a shared metaverse underpinning a safer and resilient future internet.

Governance outlook

As jurisdictions across the globe approach regulation to metaverse technologies and digital assets, intentional and impactful collaboration will be essential for the state of the future internet.

Examples of collaborative governance efforts may be:

- As described in the Safety section, the adoption of a common taxonomy of online harms will be critical to a globally successful technology governance climate.
- Globally collaborative frameworks must facilitate inclusion for and contribution by the global south.
- Governance efforts should support a common understanding of harms by developing and maintaining collaboration and information-sharing policies to ensure a broadly beneficial and rights-preserving metaverse environment.

Conclusion

The future of the internet is being built on the continued development of immersive and Web3 technologies and stands to offer transformative value to users, industries, and society.

To cultivate, advance and protect that value, it will be necessary to approach the cybersecurity and safety risks inherent to communications and financial technologies with cutting-edge expertise and global cooperation.

By focusing on resilience-minded governance efforts, stakeholders can augment traditional safety discussions and go further to ensure metaverse and Web3 advancements are broadly beneficial, equitable and sustainable.

Contributors

World Economic Forum

Judith Espinoza
Specialist, Metaverse Governance
World Economic Forum

Dylan Reim
Lead, Metaverse Governance
World Economic Forum

Daniel Dobrygowski
Head, Governance and Trust,
Centre for the Fourth Industrial Revolution
World Economic Forum

Acknowledgements

Steering Committee Members

Sincere appreciation is extended to the following steering committee members, who spent numerous hours providing critical input and feedback to the drafts. Their diverse insights are fundamental to the success of this work.

Judson Althoff
Chief Commercial Officer, Microsoft

Jeremy Bailenson
Thomas More Storke Professor
of Communication, Stanford University

Stephanie Burns
Senior Vice-President and General Counsel,
Sony

Adam Caplan
Senior Vice-President,
Emerging Technology, Salesforce

Inhyok Cha
Group Chief Digital Officer, CJ Group,
Chief Executive Officer, CJ Olivenetworks

Phil Chen
Chief Decentralized Officer, HTC-VIA

Charles Freilich
Adjunct Professor, Columbia University

Julie Inman Grant
eSafety Commissioner, Office of the eSafety
Commissioner, Australia

Marwan Bin Haidar
Executive Vice-President, Innovation and the Future,
Dubai Electricity and Water Authority (DEWA)

Huda Al Hashimi
Deputy Minister, Cabinet Affairs for Strategic
Affairs, Office of the Prime Minister of the United
Arab Emirates

Brittan Heller
Fellow, Digital Forensics Research Lab,
The Atlantic Council

Paula Ingabire
Minister of Information Communication Technology
and Innovation, Government of Rwanda

Peggy Johnson
Chief Executive Officer, Magic Leap

Nuala O'Connor
Senior Vice-President and Chief Counsel,
Digital Citizenship, Walmart

Tony Parisi
Chief Product Officer, Lamina1

Philip Rosedale
Co-Founder, High Fidelity

Robert Sherman
Vice President & Deputy Chief Privacy Officer, Meta

Yat Siu
Co-Founder and Executive Chairman, Animoca Brands

Hugo Swart
Vice-President and General Manager,
XR, Qualcomm

Artur Sychov
Founder and Chief Executive Officer,
Somnium Space

Royce Wee
Director, Department of Communications and
Connectivity, and Department of Data Protection,
NEOM Authority

Wilson White
Vice-President, Government Affairs
and Public Policy, Google

Working Group Members

This white paper is a combined effort based on numerous interviews, discussions, workshops and research. The opinions expressed herein do not necessarily reflect the views of the individuals or organizations involved in the project listed below.

Sincere appreciation is extended to the following working group members, who spent numerous hours providing critical input and feedback on the drafts. Their diverse insights are fundamental to the success of this work

Joe Abi Akl
Chief Corporate Development Officer and Managing Director of Xsight Future Solutions, Majid Al Futtaim Holding

Seokhyun Elliott Ahn
Vice-President, DT Executive Director, CDO Office and Chief Strategy Officer, CJ ONS

Anju Ahuja
Vice-President, Product Strategy and Insights, CableLabs

Saeed Aldhaheri
Director, Center for Futures Studies, University of Dubai

Flavia Alves
Head, International Institutions Relations, Meta Platforms

Ahmed Saeed Abdulla Alshami
Head, AI Systems and Services Development Team, General Directorate, Ministry of the Interior of the United Arab Emirates

Maurizio Arseni
Freelance Tech Journalist

Yoni Assia
Chief Executive Officer, eToro

Frank Badalamenti
Partner, PwC Americas

Moritz Baier-Lentz
Partner and Head of Gaming & Interactive Media, Lightspeed Venture Partners

Jeremy Bailenson
Professor, Stanford University

Avi Bar-Zeev
Founder and Chief Technology Officer, RealityPrime

Luna Bianchi
Advocacy Officer, Privacy Network

Bilel Jamoussi
Chief, Study Groups Department, International Telecommunication Union (ITU)

Gustavo Borges
Professor of Human Rights and Social Media, Department of Human Rights, University of the Extreme South of Santa Catarina (UNESC)

Sebastien Borget
Chief Operations Officer and Co-Founder, The Sandbox

Marine Boulot
Vice-President, Public Relations and Communications, Improbable Worlds

Mahmut Boz
Head, Anticipatory Regulation and Regulatory Experimentation, NEOM

Gareth Burkhill-Howarth
Global Data Protection Officer, WPP

Jehangir Byramji
Emerging Technology and Innovation, Lloyds Banking Group

Marquis Cabrera
Chairman and Chief Executive Officer, Stat Zero

Jon Camfield
Product Policy Manager, Threat Ideation, Meta

Adam Caplan
Senior Vice-President, Emerging Technology, Salesforce

Isaac Castro
Co-Chief Executive Officer and Co-Founder, Emerge

Achyut Chandra
Senior Manager and Global Lead, OI and Technology Venturing, O/o CTO, HCL Technologies

Pearly Chen
Vice-President, HTC-VIA

Phil Chen
Chief Decentralization Officer, HTC-VIA

Magda Cocco
Head, Practice Partner Information, Communication and Technology, Vieira de Almeida & Associados

Anna Maria Collard
Senior Vice-President, Content Strategy and Evangelist Africa, Knowbe4 Africa

Sandra Cortesi
Director, Youth and Media, Berkman Klein Center for Internet and Society, Harvard University

Sadie Creese
Professor of Cybersecurity, University of Oxford

William Cutler
Head, Tech Policy and Deputy to UK Tech Envoy, United Kingdom Foreign, Commonwealth and Development Office

Nighat Dad
Executive Director, Digital Rights Foundation

Julie Dawson
Chief Policy and Regulatory Officer, Yoti

Ellysse Dick
Policy Manager, Reality Labs

Eileen Donahoe
Executive Director, Global Digital Policy Incubator, Stanford

Sarah Kate Ellis
President and Chief Executive Officer, GLAAD

Liv Erickson
Innovation Ecosystem Development Lead, Mozilla

Maureen Fan
Co-Founder and Chief Executive Officer, Baobab

Nita Farahany
Robinson O. Everett Professor of Law and Philosophy; Director, Duke Science and Society, Duke University

Ellysse Dick
Policy Director, Reality Labs

Steven Feldstein
Senior Fellow, Democracy, Conflict and Governance Program, Carnegie Endowment for International Peace

Jordan Fieulleteau
Policy Manager, Reality Labs

Francesca Ginexi
Public Policy Manager, Privacy Legislation, Meta Platforms

Inbal Goldberger
Vice-President of Trust and Safety, ActiveFence

Paula Gomes Freire
Managing Partner, Vieira de Almeida & Associados

Patrick Grady
Editor of Metaverse EU, Tech Lead at Fourtold

Ashraf Hamed
Value Proposition Innovation and Pioneering, SAP

Cortney Harding
Chief Executive Officer, Friends with Holograms

Susie Hargreaves
Chief Executive Officer,
Internet Watch Foundation (IWF)

Huda Al Hashimi
Deputy Minister, Ministry of Cabinet Affairs of the United Arab Emirates

Mohamed Heikal
Head, Corporate Development, Majid Al Futtaim Holding

Vera Heitmann
Leader, Digital and Growth, Public Affairs, IKEA

Brittan Heller
Fellow, The Atlantic Council

Heidi Holman
Assistant General Counsel, Microsoft

Elizabeth Hyman
Chief Executive Officer, XR Association

Tatsuya Ichikawa
Chief Executive Officer, Avers

Stephanie Ifayemi
Global Shaper, London Hub

Rolf Illenberger
Managing Director, VRdirect

Michael Jacobides
Academic Adviser, BCH Henderson Institute, Boston Consulting Group (BCG)

Mikaela Jade
Founder and Chief Executive Officer, Indigital

Amy Jordan
Director, Technology Policy,
Office of Communications (Ofcom)

Makarand Joshi
Director, Strategy, Innovation and Standards, Schneider Electric

Tony Justman
Vice-President and Deputy General Counsel, Sony Interactive Entertainment

Lea Kaspar
Executive Director, Global Partners Digital

Stephen Kavanagh
Executive Director, Police Services, International Criminal Police Organization (INTERPOL)

Masa Kawashima
Executive Producer, Director of Asia Pacific Operations, Niantic

Hoda Al Khzaimi
Assistant Research Professor,
New York University, Abu Dhabi

Melissa Kiehl
Innovation & Foresight Advisor, ICRC

Ingrid Kopp
Co-Founder, Electric South

Ashish Kumar
Manager, Digital Strategy Office,
Ministry of Communications and Information
(MCI) of Singapore

Fabio La Franca
Founding Partner, Blueverse Ventures

Natalie Lacey
Executive Vice-President, Ipsos Media, Ipsos

Martina Larkin
Chief Executive Officer, Project Liberty

Su Kiang Lau
Executive Director, Conduct, SC Ventures, Financial Crime and Compliance, Standard Chartered

Sly Lee
Co-Chief Executive Officer and Co-Founder,
Emerge

Helena Leurent
Director-General, Consumers International

Stephanie Llamas
Principal, Metaverse Foresight Strategy,
VoxPop Insights

Dirk Lueth, Ph.D.
Co-Founder and Co-CEO Uplandme, Inc.,
Chairman OMA3 Open Metaverse Alliance for Web3

Leon Lyu
Co-Founder, Booming Tech

Kuniyoshi Mabuchi
Managing Director, PwC Japan

Deena Magnall
Director, Global Digital and Technology Policy,
L'Oréal

Noora Al Malek
Associate Project Manager, Artificial Intelligence Office, United Arab Emirates Government

Charles de Marcilly
Administrator, Council of the European Union

Eva Maydell
Member, European Parliament

Brett McDowell
Independent Chair Hedera

Dinusha Mendis
Professor of Intellectual Property and Innovation Law, Bournemouth University

Jade Meskill
Vice-President, Product, Magic Leap

Mauro Medico
Director, United Nations Counter-Terrorism Centre

Anna Miyagi
Deputy Counsellor, Secretariat of Intellectual Property Strategy Headquarters, Cabinet Office of Japan

Hiroaki Miyata
Professor and Chair, Department of Health Policy Management, Keio University

Hamdullah Mohib
Managing Director, Khas Fund, Chimera Investment

Ahram Moon
Research Fellow, Centre for AI and Social Policy,
Korea Information Society Development Institute

Steve Morris
International Chair, Portland Communications,
Omnicom

Angelica Munson
Executive Officer, Chief Digital Officer, Shiseido

Eli Noam
Professor of Finance and Economics; Director,
Columbia Institute for Tele-Information, Columbia Business School

Madan Oberoi
Executive Director, Technology and Innovation,
INTERPOL

Genki Oda
Managing Executive Officer SBI Holdings, Inc.

Reinhard Oertli
Partner, Zurich, MLL Meyerlustenberger
Lachenal Froriep

Judith Okonkwo
Founder, Imìsí 3D Creation Lab

Helen Papagiannis
Founder, XR Goes Pop

Charles Paré
Chief Integrity Officer, Head, Legal and Compliance,
World Economic Forum

Park Yuhyun
Founder and Chief Executive Officer, DQ Institute

Erin Marie Parsons
Researcher, ESADE (Escola Superior d'Administració i Direcció d'Empreses)

Kavya Pearlman
Founder and Chief Executive Officer, XRSI- X Reality

Amy Peck
Founder and Chief Executive Officer, EndeavorXR

Bertrand Perez
Chief Executive Officer, Web 3.0 Technologies Foundation

Susan Persky
Director, Immersive Simulation Program; Head, Health Communication and Behavior Unit, National Institutes of Health.

David Ryan Polgar
Founder and Executive Director, All Tech is Human

Nicola Port
Chief Legal Officer and Member of the Executive Committee, World Economic Forum

Saif Al Rahma
International Legal Advisory, Dubai Economic and Tourism Department, United Arab Emirates Government

Yonatan Raz-Fridman
Founder and Chief Executive Officer, Supersocial

Simmy Rease
Senior Legal Counsel/evision (e& life), e&

Michaël Reffay
Digital, Telecommunications and Postal Services, Permanent Representation of France to the European Union

Gina Reif Ilardi
General Counsel, Vindex

Dan Rice
Vice-President, Digital Governance, Walmart

Tim Roberts
Partner & Managing Director, UK country Co-Leader, AlixPartners

Katitza Rodriguez
International Rights Director, Electronic Frontier Foundation (EFF)

Philip Rosedale
Co-Founder, High Fidelity

Nilmini Rubin
Chief Policy Officer, Hedera Hashgraph, LLC

Erica Salinas
Principal Tech Leader, Web3, Amazon

Var Shankar
Director, Policy, Responsible Artificial Intelligence Institute

Nagwa El Shenawi
Undersecretary, Ministry of Communications and Information Technology of Egypt

Lewis Smithingham
Director, Creative Solutions, S4Capital

Ian Stevenson
Chief Executive Officer, Cyacomb

Philippe Stransky-Heilkron
Senior Vice-President and Chief Architect, Kudelski

Artur Sychov
Founder and Chief Executive Officer, Somnium Space

Kent Walker
President, Global Affairs and Chief Legal Officer, Google

Lynette Wallworth
Artist, Studio Wallworth

Alice Wang
Managing Director, Corporate and Investment Bank (CIB) Strategy, JP Morgan

Gregory Welch
Professor and Advent Health Endowed Chair in Healthcare Simulation, University of Central Florida

Deborah Welsh
Executive Manager, International, Strategy and Futures Branch, eSafety Commissioner

Josh Williams
Chief Executive Officer, Forte

Jonathan Wong
Group President, Group ONE Holdings

Samer Yaghnam
Chief Legal and Administrative Officer, Olayan

Yu Yuan
President of IEEE Standards Association, Institute of Electrical and Electronics Engineers (IEEE)

Robby Yung
Chief Executive Officer, Animoca Brands

Erez Zaionce
Director, Centre for the Fourth Industrial Revolution, Colombia

Timmu Toke
Chief Executive Officer and Founder, Wolfprint 3D

Neil Trevett
President, Metaverse Standards Forum

Paul Trueman
Senior Vice-President, Cyber and Intelligence Solutions, Mastercard

Matthew Vick
Deputy Director, Futures and Innovation, HM Revenue and Customs

Steven Vosloo
Digital Policy Specialist, UNICEF

Larry Wade
Senior Director, Crypto/BC Risk and Compliance, PayPal

Production

Rose Chilvers
Designer, Studio Miko

Laurence Denmark
Creative Director, Studio Miko

Mark Schulman
Editor, World Economic Forum

Oliver Turner
Designer, Studio Miko

Endnotes

1. Paulsen, C., & Byers , R. (2019, July). *Glossary of Key Information Security Terms*. Retrieved from National Institue of Standards and Technology: https://csrc.nist.gov/glossary/term/resilience.
2. McKinsey & Company. (2023, October 10). *What is Web 3?* Retrieved from McKinsey & Company: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-web3.
3. World Economic Forum. (2023). *Earning digital trust: Decision-making for trustworthy technologies*. World Economic Forum. https://www.weforum.org/publications/earning-digital-trust-decision-making-for-trustworthy-technologies.
4. Lyngaas, S. (2021, December 3). *Suspected Chinese hackers breach more US defense and tech firms*. Retrieved from CNN: https://www.cnn.com/2021/12/02/politics/china-hackers-espionage-defense-contractors/index.html.
5. Wyss, J. (2021, December 14). *Barbados Is Opening a Diplomatic Embassy in the Metaverse*. Retrieved from Bloomberg News: https://www.bloomberg.com/news/articles/2021-12-14/barbados-tries-digital-diplomacy-with-planned-metaverse-embassy.
6. Porter, A. (2023, 03 24). *The Costly Impact of a Data Breach on Individuals*. Retrieved from BigID: https://bigid.com/blog/the-costly-impact-of-a-data-breach-on-individuals/.
7. Price, M., Schilling , A., Treat, D., White, K., Dobrygowski, D., Espinoza, J.,Reim, D. (2024). *Metaverse Identity: Defining the Self in a Blended Reality Insight Report.* Geneva: World Economic Forum.
8. ITU Focus Group on Metaverse. (2023). *Cyber risks, threats, and harms in the metaverse* . International Telecommunications Union. https://www.itu.int/en/ITU-T/focusgroups/mv/Documents/List%20of%20FG-MV%20deliverables/FGMV-10.pdf.
9. Vivek Nair, Wenbo Guo, Justus Mattern, Rui Wang, James F. O'Brien, Louis Rosenberg, and Dawn Song. Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data. In *32nd USENIX Security Symposium (USENIX Security 23)*, 2023. https://www.usenix.org/conference/usenixsecurity23/presentation/nair-identification.
10. Financial Action Task Force. (n.d.). *Virtual Assets.* Retrieved from FATF: https://www.fatf-gafi.org/en/topics/virtual-assets.html#:~:text=Virtual%20assets%20(crypto%20assets)%20refer,many%20potential%20benefits%20and%20dangers.
11. Milmo, Dan (2024, March 11) *Bitcoin price nears $73,000 in fresh record* high: Retrieved from The Guardian: https://www.theguardian.com/technology/2024/mar/11/bitcoin-price-70000-in-record-high-cryptocurrency-crypto-fca.
12. Banusch, B. (2022, July 27) *How do non-fungible tokens create tangible value in the metaverse?* Retrieved from EY. https://www.ey.com/en_ch/technology/how-do-non-fungible-tokens-create-tangible-value-in-the-metaverse.
13. Pejic, Igor, author. Blockchain Babel: the crypto craze and the challenge to business / Igor Pejic. London; New York: Kogan Page Ltd, 2019.
14. Amazon Web Services. (n.d.). *What is blockchain technology?* Retrieved from Amazon Web Services: https://aws.amazon.com/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc.
15. Sigalos, M. (2022, February 2). *More than $320 million stolen in latest apparent crypto hack*. Retrieved from CNBC: https://www.cnbc.com/2022/02/02/320-million-stolen-from-wormhole-bridge-linking-solana-and-ethereum.html.
16. Interpol (2024) Metaverse: *A Law Enforcement Perspective*. https://www.interpol.int/content/download/20828/file/Metaverse%20-%20a%20law%20enforcement%20perspective.pdf.
17. Financial Action Task Force. (2014). *Virtual currencies: Key definitions and potential AML/CFT risks*. FATF. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html.
18. World Economic Forum. (2023). *Toolkit for digital safety design interventions and innovations: Typology of online harms*. World Economic Forum. https://www.weforum.org/publications/toolkit-for-digital-safety-design-interventions-and-innovations-typology-of-online-harms.
19. Smith, Z. L. M. (2024, February 2). *It takes a village to protect children in the metaverse*. Carnegie Council for Ethics in International Affairs. https://www.carnegiecouncil.org/media/article/protect-children-metaverse.
20. Sales, Nancy. (2024, January 5). *A girl was allegedly raped in the metaverse. Is this the beginning of a dark new future?* The Guardian. https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta?Metaver.se.
21. NSPCC. (2023, September 5). Over 75% of people believe children are at significant risk of sexual abuse when using VR technology. *NSPCC*. https://www.nspcc.org.uk/about-us/news-opinion/2023/over-75-of-people-believe-children-are-at-significant-risk-of-sexual-abuse-when-using-vr-technology.
22. Doyle, S. (2023, October 16). *Cybercrime and violent crime are converging - this is why*. Agenda. https://www.weforum.org/agenda/2023/10/cybercrime-violent-crime.
23. Heikkila, Melissa (2024, March 11) *VR headsets can be hacked with an Inception-style attack*. MIT Technology Review. https://www.technologyreview.com/2024/03/11/1089686/hack-vr-headsets-inception.

24. Vondráček, Martin & Baggili, Ibrahim & Casey, Peter & Mekni, Mehdi. (2022). Rise of the Metaverse's Immersive Virtual Reality Malware and the Man-in-the-Room Attack & Defenses. Computers & Security. 10.1016/j.cose.2022.102923. https://www.researchgate.net/publication/363857251_Rise_of_the_Metaverse's_Immersive_Virtual_Reality_Malware_and_the_Man-in-the-Room_Attack_Defenses.

25. Weimann, G., & Dimant, R. (2023). The Metaverse and Terrorism: Threats and Challenges . *Perspectives on Terrorism.*

26. United Nations Office of Counter- Terrorism . (n.d.). *The Global Programme on Prosecution, Rehabilitation and Reintegration (PRR)*. Retrieved from https://www.un.org/counterterrorism/cct/prosecution-rehabilitation-reintegration.

27. Vessali, K., Galal, H., Nowson, S., & Chakhtoura, C. (2022). *How digital twins can make smart cities better.* PwC. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.pwc.com/m1/en/publications/documents/how-digital-twins-can-make-smart-cities-better.pdf.

28. Eurasia Group (2021) *The geopolitics of the metaverse: No escaping bifurcation.* https://www.eurasiagroup.net/files/upload/EurasiaGroup_TheGeopoliticsOfTheMetaverse.pdf.

29. PR Newswire. (2022, February 8). PR Newswirse . *Arkose Labs' 2022 State of Fraud and Account Security Report Shows Online Fraud Increased 85% Year Over Year*. https://www.prnewswire.com/news-releases/arkose-labs-2022-state-of-fraud-and-account-security-report-shows-online-fraud-increased-85-year-over-year-301477191.html.

30. Global Future Council on International Trade and Investment.(2020) *The Future of Trade and Investment: A Call to Prevent Economic Fragmentation*. World Economic Forum. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www3.weforum.org/docs/WEF_GFC_Trade_Briefing_Paper.pdf.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org