NEW AMERICA

September 2023

The Forgotten "Emerging" Technology

The Metaverse and Its Cybersecurity Implications

Michael Garcia

Future Security
Last edited on September 21, 2023 at 9:07 a.m. EDT

Editorial disclosure: The views expressed in this report are solely those of Michael Garcia and do not reflect the views of New America, the U.S. government, the government offices featured in this report, or their employees.

About the Author

Michael Garcia is a senior policy advisor for the Office of Strategy, Policy, and Plans at the U.S. Cybersecurity and Infrastructure Security Agency (CISA) where he develops and supports interagency cybersecurity policies.

About New America

We are dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Future Security

Future Security is a partnership between New America and Arizona State University. It reconceptualizes U.S. security policy towards a holistic engagement with current and future challenges including domestic terrorism, armed drones, climate change, pandemics, rising authoritarianism, and new and emerging technologies.

About #ShareTheMicInCyber Fellowship

The #STMIC Fellowship, hosted in partnership between #ShareTheMicInCyber and New America, is designed to advance diversity and inclusion in cybersecurity field.

Contents

Executive Summary

The widespread deployment of 5G devices in the United States will spur increased use of augmented reality, virtual reality, and mixed reality applications —collectively known as extended reality (XR)—and they will become accessible through a single, or set of, metaverse(s). These metaverses will be a collection of virtual ecosystems that allow users to interact with each other and their surroundings in a creative and collaborative manner in virtual spaces or physical environments that are digitally manipulated by static or mobile devices.

The global XR market could be $476 billion in 2025, compared to $46.4 billion in 2019. One prediction estimates that over 23 million jobs could be created globally. While these numbers may seem a bit fantastical, future XR apps could become easily deployable and the amount of users would be significant. One estimate projects that the metaverse will increase the data usage of each internet user by 20 times.

The benefits of XR technologies could be numerous, including advanced telehealth, improved training for emergency responders, and better digital government services. For example, since 2017 a water utility in Australia has used virtual reality (VR) to allow users to walk through a virtual model of their treatment plant, helping them identify more design problems than traditional walk-throughs. More consequentially is how militaries will use XR technologies and metaverses. The U.S. military has used XR technology for decades, starting in the 1950s in which the Air Force used simulations to replicate cockpit experiences for pilots. Since then, the importance of XR technology across all U.S. military branches has only grown.

While these applications and devices will bring significant benefits, they will be accompanied by numerous cybersecurity challenges. VR headsets will introduce a host of new vulnerabilities that could allow hackers to record speech and steal sensitive information. Malicious actors could exploit XR software to look at a user's screen, turn on their microphone, and install a virus on their computer. Further, bad actors could penetrate a data-hosting provider and launch a traditional ransomware attack that encrypts data necessary for XR applications to function.

The United States must also contend with how other governments are developing policies to incentivize or regulate the XR market. The European Union published a strategic paper to detail how it will incentivize its XR market on one hand, while simultaneously initiating processes to decide how to regulate this market on the other. South Korea and Japan are investing millions to provide government services in the metaverse. More consequentially, China has created a five-year plan that details how it will become a global leader in supplying the XR

technology supply chain and is taking steps to lead in international standards conversations and integrate XR technology into their military operations.

Compared to China and other countries, the United States is woefully behind in establishing any policies to incorporate XR technologies into society, let alone dealing with its cybersecurity concerns.

The U.S. government has issued several strategies on national security, emerging technology, and cybersecurity that could impact the security of XR technologies. However, they do not explicitly mention XR or the metaverse nor are there any major government or congressional activities underway to address this risk.

The U.S. government must work closely with industry, academia, nonprofits, and international partners to begin thinking about these consequential issues. This should include: encouraging XR companies to adopt security frameworks and standards; becoming involved in developing international standards; examining existing and new regulations that could apply to XR; and determining how, if at all, the U.S. XR market should receive financial incentives, among other things.

Introduction

The first iPhone was released in 2007 and 4G connections rolled out a year later. With the wide scale adoption of smartphones and accessibility to 4G, mobile applications took off. Yet, the cybersecurity implications were not thought of until the incidents started occurring. Few raised alarms about foreign interference in elections by manipulating social media. The sale of American data to unregulated data brokers that can then be bought by law enforcement agencies was one of a dystopian future. The widespread use of Bitcoin, first developed in 2009, and the thousands of virtual currency iterations since then helped give rise to devastating ransomware attacks. And with the return of great power competition, the United States and its allies had to confront the daunting challenge of ensuring the semiconductors, software, and hardware underpinning the technology of the 4G-tech ecosystem were free from adversarial malfeasance. All these issues were brought on, more or less, by the onset of 4G devices and applications.

With the deployment of 5G towers and cells throughout the United States, 5G-capable phones and devices will increasingly proliferate. But the true benefits of 5G will be those technologies that take advantage of reduced up/down data streams, especially those using augmented reality, virtual reality, and mixed reality applications—collectively known as extended reality (XR). These applications will become accessible through a single, or set of metaverses, which will allow users to engage with a near-infinite number of XR applications. These metaverses will be a collection of virtual ecosystems that allow users to interact with each other and their surroundings in a creative and collaborative manner in virtual spaces or physical environments that are digitally manipulated by static or mobile devices.

The benefits of these metaverses and the associated XR technologies could be numerous, including advanced telehealth, improved training for emergency responders, and better digital government services. Importantly, XR technology is not necessarily an emerging technology, but one that has been around for decades. Indeed, the U.S. military has relied on XR technology since the 1950s to train fighter pilots and to help them navigate the skies.

While these applications and devices will bring significant benefits, they will be accompanied by the cybersecurity challenges that pervaded the 4G ecosystem. These same cybersecurity challenges will be compounded due to the increased amount of data produced by the metaverse and a broader attack surface for malicious cyber actors to exploit. Cybersecurity practitioners will once again be confronted with data privacy concerns, online radicalization, mis-dis-mal-information, disruptions to critical infrastructure, virtual currency theft, digital identity management challenges, and supply chain disruptions. The security of the technology comprising the headsets and other devices that enable access to

the metaverse, and the origin of XR apps themselves, will become a topic of concern. Just as the United States and Western nations are concerned with Chinese apps and information and communications technology products today, the same will hold true for XR applications as China increasingly seeks to be a leader in this field.

Unfortunately, the over-commercialization of the term "metaverse" has impeded honest conversations about the implications of an insecure metaverse and the technologies associated with it. As a result, U.S. policymakers run afoul of repeating past mistakes: failing to secure technology before it ushers in a new era of national security concerns.

What is the Metaverse?

Words Matter: Defining the Metaverse

A core challenge of identifying tangible problems and solutions for the metaverse and the technologies associated with it is the numerous concepts and definitions that define it. Having a clear definition of the metaverse that applies to a wide range of circumstances helps identify the technology that enables it and facilitates conversations on the opportunities and challenges.[1] While experts agree that the term "metaverse" originated in 1992 from the science fiction book *Snow Crash*, agreements on what constitutes the metaverse tend to end there.[2] *Snow Crash* describes the metaverse as "a wireless internet system with three-dimensional graphics and a virtual reality, which was populated by digital avatars of real people and accessible via terminals on a worldwide fiber-optics network using special goggles."[3] Despite how eerily accurate this definition captures current aspects of the metaverse, a wide range of definitions still exist. For instance, Matthew Ball, the author of *The Metaverse: And How It Will Revolutionize Everything*, provides a robust definition describing the metaverse as "a massively scaled and interoperable network of real-time rendered 3D virtual worlds that can be experienced synchronously and persistently by an effectively unlimited number of users with an individual sense of presence, and with continuity of data, such as identity, history, entitlements, objects, communications, and payments."[4] A report from the cybersecurity company Trend Micro defines it as "a cloud-distributed, multi-vendor, immersive-interactive operating environment that users can access through different categories of connected devices (both static and mobile)."[5] And researchers from South Korea define it as "an immersive network of socially connected environments in a persistent multi-user platform."[6]

One primary theory for the differing definitions is that it is in businesses' interest to keep them vague and confusing. RAND scholars recently concluded that companies offer various definitions "often slanted to suit their own needs,"[7] as companies cannot fail in creating business products if the shareholders do not know its purpose. Matthew Ball also explains that these numerous definitions are intentionally at odds with each other.[8] While advantageous for businesses, vague definitions impede policymakers and subject matter experts from working on complex metaverse issues.[9]

Although companies have created their own definitions to suit their business needs, the U.S. government has not offered a definitive view on what they consider the metaverse. The Congressional Research Service (CRS) describes concepts and defines other key terms in their published reports on XR, but they do not provide a distinct definition.[10] Similarly, the National Institute of

Standards and Technology's (NIST) Computer Security Resource Center's Glossary does not contain a definition for "metaverse." This is because NIST only defines terms that are included in their publications, meaning that NIST has not developed products mentioning the metaverse (though they have other lines of effort in this field that will be discussed later).[11]

In lieu of a uniform definition, frustrated researchers have attempted to solve this dilemma. Georg Ritterbusch and Malte Teichmann wrote a paper for the Institute of Electrical and Electronics Engineers (IEEE) detailing their literature review to uniformly define the "metaverse." Based on their analysis of 28 prominent definitions, they conclude "the metaverse, a crossword of 'meta' (meaning transcendency) and 'universe,' describes a (decentralized) three-dimensional online environment that is persistent and immersive, in which users represented by avatars can participate socially and economically with each other in a creative and collaborative manner in virtual spaces decoupled from the real physical world."[12]

Yet, even this definition has limitations because it claims that the metaverse must be "decoupled from the real physical world," which overly restricts the applications and types of technology that comprise the metaverse. Other definitions also exhibit this shortcoming except for the definition in Trend Micro's report, which, as previously detailed, describes the metaverse as "immersive, digital environments" that can be accessed through "static or mobile devices."[13] In other words, the metaverse should be more expansive than only a virtual environment that can only be accessed through a virtual reality (VR) headset. The metaverse ecosystem should also include technologies that comport physical reality by overlaying digital images or digitally manipulating an environment.

The metaverse could therefore be thought of as a spectrum of how a user manipulates their environment: with full digital immersion at one end and a smartphone's camera filter that places a virtual sofa in a physical living room on the other. To drive this home, a user does not need to be completely submerged in a virtual environment to access the metaverse. Operating off this reasoning, a revised definition of the metaverse could be the following: **The metaverse is a blend of online environments that is persistent and immersive, in which users can participate socially and economically with each other and their surroundings in a creative and collaborative manner in virtual spaces or physical environments that are digitally manipulated by static or mobile devices.** This then erodes the notion that someone can only access the multiverse through a VR headset, but also through a variety of XR devices and applications.

That naturally leads to the need to define XR and identify technologies within the XR family. XR could be defined as the extension of the reality perceived by users, referring to any technology that can alter reality by adding digital elements to the

user's environment.[14] This includes a range of technologies that enable VR, augmented reality (AR), and mixed reality (MR). VR provides the user with a wholly virtual and immersive visualization,[15] while AR is "technology that overlays digital information to the real world through a screen or surface onto which the digital information is projected or shown."[16] In other words, AR provides an "enhanced version, not a replacement, of a user's perception of physical reality."[17] MR is a mix of VR and AR and offers a "highly interactive AR application, where virtual objects realistically blend into and interact with, real objects and/or with the user and allows the user to interact with both digital and physical elements."[18]

With the metaverse defined and the technology to access it identified, the third leg of this three-legged stool is the technology ecosystem that allows for the metaverse to operate. First, there is the primary technology that the user directly interacts with. This includes headsets, mobile devices, sensors, virtual applications, computers, and other tools that allow the user to directly access the metaverse.[19] The secondary technology includes those that enable the users' devices to function properly. This includes cloud computing that hosts data produced during a user's session, the semiconductors within headsets, and the third-party code that a metaverse or XR app relies upon. The third tier consists of technologies that enable the internet, such as 5G cell towers and fiber optic cables. While this is not an exhaustive list, this framing shows how the attack surface that a malicious actor could exploit will expand with the use of XR technology and how they could exploit existing infrastructure to impact XR technology.

Follow the Money

Similar to the challenge of defining the metaverse, economists also struggle to understand the metaverse and XR technologies' impact on the economy. For instance, PwC suggests that the global XR market will be $476 billion in 2025, up from $46.4 billion in 2019.[20] A coalition of XR companies in the European Union (EU) believes that the EU can see an impact ranging from $838 billion to $1.5 trillion by 2030.[21] McKinsey is more optimistic and believes that the "economic value of the metaverse" could have a $5 trillion impact by 2030.[22] Of course, knowing what is defined as the "metaverse" and what is considered a "metaverse technology" impacts these economic estimates. There is also varying economic growth across different sectors. For example, in another McKinsey report, e-commerce may see an impact of $2 trillion to $2.6 trillion from XR technology, $180 billion to $270 billion in the academic virtual learning market, a $144 billion to $206 billion impact on the advertising market, and a $108 billion to $125 billion impact on the gaming market.[23]

While these numbers may seem bloated, business investments and market trends favor these estimates, despite the recent quarterly market downturns in XR technology. The number of mergers and acquisitions throughout the years has increased from 109 in 2018 to 166 in 2020.[24] Andreessen Horowitz operates the cleverly named "Games Fund One," a $600 million fund investing in "game studios, metaverse infrastructure, and games themselves."[25] Overseas, total equity fundraising in U.K. companies was roughly $3 billion between 2018 and 2022.[26] These investments have the potential to translate to job creation, with the EU expected to create anywhere between 440,000 to 860,000 jobs by 2025.[27] One prediction estimates that over 23 million jobs could be created globally.[28]

Regardless of the true economic impact, these companies and investors clearly believe that if they build it, (or more aptly, invest in it), users will come. A survey in 2022 found that 62 percent of respondents engaged with branded virtual experiences, 36 percent were excited about brands in the metaverse, and 30 percent were excited about luxury brands providing products in the metaverse.[29] In 2026, a quarter of the world population could spend "at least one hour a day in the metaverse for work, shopping, education, social and/or entertainment."[30] Indeed, a recent Pew survey of developers, business leaders, researchers, and activists found that 54 percent believe that by 2040 the "metaverse will be a much more refined and truly fully immersive, well-functioning aspect of daily life for a half billion or more people globally."[31]

Understanding the number of users that could use XR applications also demonstrates just how widespread using the metaverse could become, and, by extent, the data its users will produce. Today, Americans from 16 to 64 years old spend an average of seven hours a day online.[32] If that trend holds, or more likely expands, they will eventually spend their time online in various metaverses. The data generated per day, per week, per month, and per year then starts to become an unimaginable, but very real, number that companies and governments must contend with. One estimate projects that the metaverse will increase the data usage of each internet user by 20 times.[33]

Due to these economic estimates, the current high internet usage rate, and new data generated, C-Suite executives are optimistic about incorporating XR technology into their businesses. In a recent survey, a near-unanimous 95 percent of senior executives "expect the metaverse to have a positive impact on their industry within five to ten years."[34] As a result, these executives believe this technology will have a positive impact on their economic bottom line. Sixty-five percent expect metaverse technology to influence more than 5 percent of their total revenue in five years, while 24 percent take a more optimistic view and think it will drive more than 15 percent of their revenue.[35]

These surveys have translated into real-world market movements, with big-name companies taking steps to get into the metaverse market. While Microsoft's $69

billion acquisition of Activision would help cement its place in XR and video games, they also created "Mesh" to enable teams to better connect with each other in virtual environments.[36] Google released "ARCore Geospatial API," which provides "immersive" experiences within Google Maps in over 100 countries.[37] The rock band, Gorillaz, famously used this platform to perform an AR concert in 2022.[38] The Chief Technology Officer of Roblox remarked in 2023 how they are making investments to ensure that Roblox manifests a "build once, run anywhere" system so that a Roblox experience "can run on a high-end PC, … run on a three-generation-old phone, [and] run on a VR headset or a console."[39] A quick search for the term "metaverse" in the SEC's Electronic Data Gathering, Analysis, and Retrieval system reveals over 5,000 documents between July 2018 to July 2023.

Source: YouTube/Gorillaz

Despite its promise, the market is constantly fluctuating. The company most directly associated with the metaverse, Meta, has seemed to completely pivot to artificial intelligence.[40] Disney shut down its entire metaverse division.[41] While these may indicate that XR technology is a fad that will never gain traction outside of the gaming industry, the following case scenarios illustrate that as XR technology becomes cheaper and more easily accessible their applications could become limitless.

How Will the Metaverse Be Used?

XR technology has the potential to be, if not already, integrated into a wide range of business and critical infrastructure sectors. The video game industry is probably most closely associated with the metaverse and how someone is likely

to come into contact with XR technology. For example, accessing Pokémon GO, a form of AR, only requires a smartphone, connection to the internet, and access to an application store. At its peak in 2016, Pokémon GO was estimated to have 232 million active users.[42] Unsurprisingly, in Europe, VR/AR videogames were the largest source of earnings for all XR technologies in 2022, representing about €11 billion.[43]

Beyond video games, the adoption of "digital twins" can expand the use of metaverses. Digital twins are "digital copies of actual surroundings and digital avatars representing real users that are created for virtual world experiences."[44] An individual's digital twin could, theoretically, do everything virtually that the user could do in the real world. Within retail, customers could use their digital twin to try on clothes or, in a Sims-like fashion, see how a piece of furniture or art may look in their house. For critical infrastructure, a digital twin could be used to train workers in operational technology environments by using digital schematics without the stress of making a costly mistake.

In fact, metaverse applications could be used in all 16 U.S. critical infrastructure sectors.[45] These 16 sectors consist of "assets, systems, and networks, whether physical or virtual, [that] are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[46] Therefore the security and resilience of these sectors are of the utmost importance to the U.S. government and the owners and operators of these systems and assets. Although the following use cases illustrate the benefits XR can bring to these sectors, they also exemplify the need to ensure that these systems are secure from cybersecurity threats:

- **Water and Wastewater:** Since 2017, a water utility in Australia has used VR to allow users to walk through a virtual model of their treatment plant to help identify more design problems than traditional walk-throughs.[47]

- **Dams:** The U.S. Army Corps of Engineers is identifying AR/VR solutions to help with flood risk management infrastructure.[48]

- **Transportation Systems**: XR can be used for passenger airplane flight deck training to simulate emergency landing situations.[49]

- **Financial Services:** Citigroup launched a "virtual trading desk" with Microsoft HoleLens to allow a user to view a digital workstation showing stock performances and other market information.[50]

- **Food and Agriculture:** A startup called Plant Vision allows farmers to use headsets to get information about their crop's temperature, health,

and other vital information by leveraging various infrared cameras and sensors.[51]

- **Health Care and Public Health:** Medical professionals can train in realistic scenarios, improve telehealth appointments, enhance medical imaging, and allow professional surgeons around the world to assist with any given surgery. For example, the European Tampere University leads a research consortium to identify how to present medical imaging data in combination with 3D methods.[52]

- **Nuclear Reactors, Materials, and Waste:** Headsets or AR-visors could superimpose information about the radiation source strength in a power plant, helping prevent unintended exposure to employees.[53]

- **Communications:** With limited inspectors available after a major storm, telecommunication providers can dispatch personnel with XR headsets to inspect damaged cell towers and connect with inspectors who can then walk the dispatch personnel on how to repair the damages based on a tower's digital twin.[54]

- **Emergency Services:** Trainees from emergency services, fire, and police departments could be placed in virtual environments to simulate terrorist attacks, an incident at a large public gathering, and other natural disasters to help train emergency response plans.[55]

- **Government Facilities:** U.S. cities could create digital twins of municipal services to allow citizens to access and process government requests in a replica of a city in a metaverse environment, similar to the efforts underway in Seoul (further detailed later in this report).

- **Commercial Facilities:** As previously described, stores can revolutionize online shopping by allowing customers to interact with their products through various XR applications.

- **Critical Manufacturing:** XR could improve the accuracy and efficiency of drilling by connecting off-site specialists with those operating the drilling platforms and tools.[56]

- **Chemical:** Similar to the medical field, scientists can simulate environments where chemicals could be safely stored in various conditions to find better efficiencies.

- **Energy:** AR headsets could be clipped onto hard hats that technicians wear during pipeline inspections to project instructions for the technician, which could reduce errors.[57]

- **Information Technology:** The XR companies that create metaverse ecosystems and related devices and cloud companies hosting user data would fall within this sector. While IT companies could use XR applications similarly to other sectors, their greatest impact would be in supporting XR technologies.

The most consequential use of XR technology is how the 16th sector, the Defense Industrial Base Sector, will deploy it to support military organizations to train soldiers and carry out military operations. In the United States, XR technology has been used in the military for decades. The U.S. Air Force began using flight simulators as early as the 1950s to replicate cockpit experiences for pilots.[58] In the 1980s there was SIMNET, which was a "wide-area network with various vehicle simulators built to provide a real-time, distributed combat simulation."[59]

Since then, the importance of XR technology across all military branches has only grown, and senior leaders within the Department of Defense (DoD) have increasingly spoken to its importance. Dr. Alethea Duhon, the Technical Director at the Air Force Agency for Modeling Simulation, remarked that "VR and augmented reality technologies are of huge importance in the way we innovate moving on because that's what this generation is used to. Technology is catching up. We cannot slow down."[60] Lisa Costa, Space Force's Chief Technology and Innovation Officer, noted that they should "take advantage of the investments that industry is going to be making in the metaverse. Those technologies could be used for training as well as for operations. And incorporated into a digital engineering ecosystem, operator feedback could be used to automatically improve the product in its next iteration."[61] The Under Secretary of Defense for Research and Engineering Heidi Shyu said that the DoD intends to leverage "AR/VR and live training…[that is being matured] by the gaming industry" to develop DoD XR programs.[62] Those remarks came on the heels of her office identifying "human-machine interfaces for XR as one of 14 critical technology areas for the Department of Defense."[63]

These are not merely words, as the DoD has increasingly leaned into XR to fulfill its training needs. For example, the DoD's Army's Synthetic Training Environment (STE) is an XR training environment that allows soldiers "to train where they will fight, with the partners they will fight with, and in complex operational environments to include dense urban, woodland, jungle, desert, and sub-terrain, before the first fight begins."[64] In practice, the STE will enable "mission rehearsal capability, [as it] interfaces with operational networks, training interfaces with battlefield platforms, interfaces to live training instrumentation, and native interoperability with the Common Operating

Environment."[65] One example of how this will look is the STE Information System (STE-IS) and the Reconfigurable Virtual Collective Trainer (RVCT). The former uses a 3D mapping dataset that "integrates actual terrain imagery from around the world" to enable training scenarios in those locations.[66] The RVCT is an interactive set of equipment (e.g., head displays and representational controllers) that will allow soldiers to train in Abrams, Bradleys, and Strykers in an STE-IS environment.[67]

The STE is just one of many examples of XR military training across different military branches. In addition to the STE, the Army developed the Virtual Squad Training system in Hawaii to simulate tactical training for squads such as performing combat patrols, entering and clearing buildings, and reacting to IEDs.[68] In 2014, the Office of Naval Research partnered with the University of South California to develop "Project BlueShark" to provide a virtual environment for sailors to train on vessels and virtually collaborate.[69] The Navy launched the "Naval Aviation Training Next-Project Avenger" to "reduce the length of time it takes to train students by combining traditional classroom instruction and flying time in the T-6B Texan II with virtual and mixed-reality trainers, artificial intelligence, tablets, and aviation apps."[70] The Air Force is also interested in creating an XR environment for maintenance training and creating virtual training hangars.[71]

XR technology can also enable large-scale military exercises with global partners that otherwise would be costly. CRS found that performing XR-enabled military exercises could save costs and protect military personnel from otherwise dangerous activities while maintaining the ability for multi-state units to exercise together.[72]

In addition to training and exercises, the military increasingly uses XR technology on the battlefield. Air Force pilot helmets for years had aspects of XR that enabled pilots to better navigate and manipulate their environments. The helmet for the F-35, for example, includes an AR display that shows telemetry data and target information over video footage from around the aircraft.[73] In 2018, the Army gave $22 billion to Microsoft to develop the Integrated Visual Augmentation System (IVAS), which is a headset to "improve soldier sensing, decision-making, target acquisition, and target engagement," and will eventually be incorporated into both ground and air vehicle platforms.[74] Additionally, the Army has developed Tactical Augmented Reality goggles that combine traditional GPS devices and night-vision goggles so that soldiers do not have to look down at their GPS device.[75]

This is not to say that these programs do not have their challenges. Those who use XR technologies in daily operations may grow too reliant on their systems, leaving them at a disadvantage if a disruption were to occur. Similarly, the user may be paralyzed into inaction due to information overload.[76] Securing the data

produced in the training environments will also increasingly be a challenge. A recent CRS report has begun raising alarms, highlighting "concerns about the potential cybersecurity vulnerabilities of XR systems, particularly those that rely upon high-value-target databases for weapons maintenance, image classification, or other functions."[77] In terms of the impact on the military, CRS assesses that: "If such systems are infiltrated, they could provide an adversary with critical information about U.S. weapons systems, as well as information about how the U.S. military trains, and thus how it intends to fight in the event of a conflict. XR systems used for warfighting could additionally enable an adversary to distort the common operational picture used to coordinate military actions or cause the system to misidentify people and platforms—potentially resulting in fratricide or unintended civilian casualties."[78]

Cybersecurity and the Metaverse

While much has been written about the opportunities of the metaverse, less has been written about the cybersecurity risks that come with it. Malicious actors can exploit vulnerabilities in XR hardware and software to compromise the confidentiality, integrity, and accessibility of the data or functions of an XR program. Compromising an XR technology will be just another means for bad actors to perform ransomware attacks, steal intellectual property, or disrupt National Critical Functions.[79] National security and cybersecurity practitioners must also determine whether a new novel cyber attack could be launched through XR technologies. And this is not to mention other security concerns that will stem from the use of XR technologies, such as the spread of mis-, dis-, and mal-information, theft of virtual currencies, online radicalization challenges, and data privacy concerns. While this section will focus on how bad actors can impact the confidentiality, integrity, and accessibility of XR and associated technologies and touch on data privacy concerns, national security practitioners must also be cognizant of other security concerns that will surely arise with the use of metaverses.

Hardware

Today's hardware devices, such as a headset or someone's smartphone, tablet, or laptop, are what allow users to access a metaverse. While much is understood about the security vulnerabilities of the latter, the increasing proliferation of headsets adds new capabilities and vulnerabilities that previous devices were limited in. For instance, headsets can capture the user's vocals, audio sounds in the room, retinal movements, user location, orientation, body movements, and a 3D mapping of the user's environment.[80] Peeking inside the headset reveals the same underlying supply chain issues that have plagued other information and communications technologies, particularly semiconductors. The same chips powering our phones, computers, cars, and other interactive technologies are the same ones found in these headsets. Policymakers have implemented a slew of policies to address the semiconductor supply chain, but there may be a slew of new supply chain issues with headsets, such as the near-eye displays on the headset. China, for instance, has detailed in a new five-year plan that it would like to become a global supplier of these displays.[81] This inevitably opens the door for new supply chain attacks and disruptions.

VR headsets will introduce a host of new vulnerabilities to an IT environment that will be a massive headache for the chief information security officer of any organization, let alone an individual consumer. The Augmented Reality for Enterprise Alliance (AREA) sums it up best by saying "Augmented Reality headsets open up new, unique, and significant threat potential to enterprise

assets. They represent doorways through which bad actors can surveil, infiltrate, and potentially commandeer and misdirect critical resources and function."[82] Their reasoning for this is that no one wants to own the security problem for the headsets. As they put it: "There is a tendency for stakeholders to 'pass the buck' when it comes to taking responsibility for AR security: device vendors say it is the responsibility of the customer and can probably be handled by (mobile device management) MDM applications; MDM providers have not seen enough deployments to extend their platforms to meet AR-specific needs, which would not be sufficient in any case; AR project teams look to Enterprise IT for guidance; Enterprise IT and Mobility departments hesitate to open up their networks to these devices [and then do not develop guidance]."[83]

The lack of ownership is troublesome given the discovery of vulnerabilities in these headsets. A team at Rutgers University found that hackers could infiltrate a headset and "record subtle, speech-associated facial dynamics to steal sensitive information communicated via voice command, including credit card data and passwords."[84] Their research focused on vibrations captured by AR/VR headsets, such as "speech-associated facial movements, bone-borne vibrations, and airborne vibrations." While seemingly innocuous, these vibrations could reveal detailed gender, identity, and speech information. These vulnerabilities could also allow bad actors to commit eavesdropping attacks, thereby enabling them to "derive simple speech content, including digits and words, to infer sensitive information, such as credit card numbers, Social Security Numbers, phone numbers, PIN numbers, transactions, birth dates, and passwords."[85]

Security practitioners must also account for where and how these headsets are used. Compromised headsets used for video games present different risk levels than headsets used for educational, medical, or military purposes. Yet, the individual parts comprising the headsets may be ubiquitous across the headset ecosystem—regardless of the final assembler of the headset—and the discovery of a vulnerability in any given headset could have ramifications across multiple sectors.

Software

Malicious actors could also exploit XR software to achieve their goals. A research team at Louisiana State University (LSU) found that bad actors could compromise a popular social and entertainment XR app and "take over a user's VR headset, look at their screen, turn on their microphone, and install a virus on their computer."[86] The vulnerability also allowed any hacker to join private rooms, download additional malware on a user's system, phish additional users, and send messages from a user's account.[87] Further, users interacting with the "infected" individual also caught the computer virus, facilitating a virtual pandemic.[88] It is easy to imagine a scenario in which a bad actor extorts a victim

by recording private sessions and interactions and threatens to release information unless ransoms are paid.[89] Even the most sophisticated and well-resourced companies are not immune from these potential cyber incidents. Security researchers found multiple vulnerabilities in Roblox that, if exploited, could unveil names and email addresses to millions of users.[90]

Regardless of the software manufacturer, malicious actors will likely find a way into the system and perform various types of cyber attacks. This includes launching an input attack that would prevent authorized commands from being recognized, making it impossible for users to operate in the metaverse. An adversary can launch a distributed denial of service attack and overload the system, resulting in network failures. Similarly, bad actors can perform a feedback overload attack that causes delays in information transmissions. An attacker could also overlay images into an environment "making it seem like new elements have been added or removed" or block the view in its entirety.[91] The consequences of delayed or falsely overlaid information can be fatal during, for example, a medical operation that relies on XR capabilities.[92]

The authentication methods used to access a metaverse could also be corrupted or stolen, allowing unauthorized access or denying users' access to their environment. But not all authentication compromises are created equal. A gamer's inability to access Fortnite may not warrant a U.S. government response (much to the chagrin of the gaming community), but a soldier's inability to train in STE may be of significant concern. Some XR devices, similar to smartphones and headsets, can only be accessed through certain biometrics, introducing another vector to capture this important piece of identity information. As airport security increasingly turns to facial recognition for screenings, for example, the integrity of someone's facial biometrics is of vital importance.

Moreover, bad actors do not need to exploit a headset or the XR software to successfully impact an XR application. They could penetrate a data-hosting provider and launch a traditional ransomware attack that encrypts data necessary for an XR application to function.[93] As a result, end users, like hospitals or the military, may lose the essential operational functions of their XR applications. In addition to ransomware, bad actors can steal user data from a cloud provider, corrupt data so that the XR application shows incorrect information, delete data, and provide a launch point to enter the XR environment or the user's larger IT ecosystem.

New Cyber Threats

While a hacker could use an existing attack method to inflict pain on a victim, they could also exploit new vulnerabilities within XR technology. This could include corrupting a digital twin, stealing virtual currency, or physically manipulating a user. A user's avatar, or digital twin, could become corrupted or

altered to an extent that makes it unusable.[94] While defacing someone's avatar may not seem like a national security threat, the mental and emotional toll on the user should not be overlooked. At a larger scale, if a city, such as Seoul, were to have its digital twin corrupted it may actually limit government services for its citizens. Although government services could still be requested in-person, the intent should be recognized for what it is: inflicting real-world consequences by debilitating the government's ability to provide basic functions to its citizens. Taking this a step further, a power plant or water utility could create a digital twin of their plant with schematics to help with equipment and sensor monitoring. A malicious actor could gain unauthorized access to that digital twin and could preplan physical or cyber attacks based on those digital schematics.[95]

One of the more unique outcomes that a bad actor could achieve is physically manipulating the user. Unlike most interactions with internet-enabled devices, XR technology's primary purpose is to alter the reality of the user and to allow the user to interact in the metaverse by physically moving their bodies. As a result, a bad actor may seek to physically harm the user through a cyber attack. This has ominously been dubbed the "human joystick" phenomenon. In an IEEE study, they found that "87.5 percent of subjects were able to have their movements controlled by the addition of supplementary content to their VR screen... malicious software might add additional 'objectives' or mechanics to games that induce the user to move in a particular direction."[96]

Unfortunately, these vulnerabilities already exist. In the same study where the LSU research team hacked a headset through an XR application, researchers also found that they could "disorient users and delete physical boundaries to make them walk into walls or fall down staircases in reality."[97] Another research team analyzed metaverse applications, systems, and traffic flow and found that an attacker could "easily mimic and visualize the immersive environment of the victim." This could then lead to "integrity violations, content tampering, and the obstruction of users' views" and cause "cybersickness."[98] This phenomenon has already occurred in the real world when Pokémon GO reached its peak and criminals began abusing the game's functionalities to prod gamers to walk into certain areas where they would get robbed of their belongings.[99]

Privacy

All of the aforementioned vulnerabilities and exploits touch on various aspects of users' and organizations' privacy. In fact, there are several thoroughly detailed reports that focus on all aspects of privacy, and one literature review of "metaverse security" reports found that "most articles have examined the security of Metaverse environments from a privacy-preservation perspective."[100] These concerns are not misplaced, as XR applications will produce sensitive data about users that have previously not been generated—and they are ripe for the

taking. The IEEE has published several reports on the matter and highlighted four key data captures that XR enables malicious actors to access that include movements and physical actions, neural activity, location tracking, and physiology.[101]

This personal data does not include other information associated with a user or organization and is in addition to existing data tracked by basic internet use such as login credentials, personal identifiable information, financial information, or health information.

XR systems, like other technologies preceding it, will be targets of criminals and nation-state cyber attacks. The integration of XR systems and the data it produces becomes another opportunity on a widening attack surface. A criminal will deploy ransomware on a managed service provider (MSP) if they know it hosts the data for hospitals that cannot function without it. A nation-state actor may try to pilfer data from a server hosting DoD information that is generated from a fighter pilot's XR headset to learn about an exercise that occurred in the South China Sea. Other malicious actors could preposition malware on an XR application that is widely used for the functioning of critical infrastructure operations in the United States and deploy it if hostilities were to increase. While the likelihood of these scenarios occurring varies, and their impact is dependent upon the integration of the XR device or application in a business unit, the U.S. government and private sector must be mindful of these legitimate cases.

Global Stakes of Extended Reality

From the European Union (EU) to the United Kingdom (U.K.) to South Korea, government institutions are taking unique approaches to stimulate, integrate, and regulate their burgeoning XR markets. China, too, wants to support its XR market and incentivize using the metaverse across various sectors, but also wants to become a dominant player in controlling the XR supply chain and international standards. This could have significant national security concerns, especially as the United States and its allies turn towards metaverse applications to support critical infrastructure and military operations.

European Union

The EU has one of the more comprehensive approaches to integrating XR technologies into European society and economy by fully embracing an all-inclusive technology strategy and metaverse-specific plans. In December 2022, the EU released the "European Declaration on Digital Rights and Principles," detailing six core principles that will guide the EU's approach to all aspects of technology, including XR. One of these principles, "safety, security and empowerment," includes commitments to:

- Protecting the interests of people, businesses, and public institutions against cybersecurity risks and cybercrime, including data breaches and identity theft or manipulation. This encompasses cybersecurity requirements for connected products placed on a single market;
- Ensuring that everyone has effective control of their personal and non-personal data in line with EU data protection rules and relevant EU laws;
- Protecting communications effectively from unauthorized third-party access; and
- Countering and holding accountable those that seek to undermine the security and integrity of the digital environment or promote violence and hatred through digital means.[102]

The EU is also creating metaverse-specific policies and establishing new forums to help inform government policies. In 2020, the European Commission launched the Virtual and Augmented Reality Industrial Coalition to bring together EU policymakers and VR/AR companies. Through this coalition, the EU has held over 100 workshops from 2021 to 2022, developed a roadmap detailing how the EU should operate and invest in XR technologies, and published a

strategic paper assessing the XR market in the EU.[103] This strategic paper outlines several roles for the government to strengthen the market, including:

- Increasing the number of small funding opportunities by broadening application requirements, simplifying application procedures, reducing red tape, and increasing accessibility of those by all types of stakeholders active in VR/AR development;

- Acting to make large financing opportunities available to support risk-taking and scaling-up of companies; and

- Educating investors by collecting and making available market data and trends regarding the adoption and growth of the technology.[104]

Despite the robust nature of the strategic paper, it shirks the importance of securing the metaverse. In a section on the "most important challenges/ opportunities facing the EU VR/AR sector" the term "security" is the last item placed under "legal" with a "medium" impact if it is not addressed.[105] In fact, the word "security" only appears 21 times in the 117-page document.[106] Despite this, the EU acknowledges that they need to ensure the metaverse is safe and secure for Europeans, expressing that "the metaverse platforms pose significant privacy-related challenges."[107] Specifically, there are concerns about whether any regulatory regime can keep pace with the amount of data generated and whether existing regulations are applicable to the metaverse.[108] For example, the General Data Protection Regulation may not cover the "invasive forms of data collection" that some XR technologies may create and store.[109]

Realizing the limitations of existing regulations, EU officials have taken several steps to begin shoring up this gap. The European Commissioner for the Internal Market, Thierry Breton, announced in 2022 that "private metaverse spaces should be based on interoperable standards," including data interoperability standards that give consumers better control of their data.[110] He went on to mention that the Digital Services Act (DSA) and Digital Markets Act (DMA), two key laws that regulate the internet, provide Europe with "regulatory tools for the digital space," but did not go into detail as to how they would apply to the metaverse.[111] Other types of regulations include network infrastructure taxes that will tax network providers, new digital rules to implement the DMA and DSA in the metaverse, and additional safety and interoperability measures.[112] As in other emerging technologies, such as artificial intelligence, the United States should pay attention to how the Europeans leverage regulation to control the metaverse and its impact on the EU market.

United Kingdom

A stone's throw away from the EU's domain, the U.K. has worked closely with the private sector to take advantage of what the metaverse has to offer. The greatest effort was a large-scale consultation in 2022 in which the U.K. government put out a request for information on the opportunities and challenges of a "national cyber-physical infrastructure" that includes digital twins, robotic and autonomous systems, Internet of Things devices, and AR/VR technologies.[113] The UK government stated that: "[W]e care because [cyber-physical technology] is coming and it is incumbent upon us to play an active role in how that happens; there will be risks emerging as part of this that we need to address; there are significant opportunities for the U.K.'s society and economy; and we have received a clear call from key players in the ecosystem to take an active role."[114]

Commenters agreed that "core" sectors would stand to benefit from cyber-physical infrastructure such as "energy systems and utilities; infrastructure and built environment; manufacturing; natural environment; transport and supply chains; and wellbeing, health, and social care."[115] But they also called out key areas where the government could address "systemic challenges" by supporting "key enablers" including security and resilience; interoperability; recognized value propositions; frameworks, guidance, and standardization; and skills.[116] Specifically, these commenters would like the U.K. government to:

- Launch a grant competition to fund one or more organizations working together to develop and host a cyber-physical infrastructure ecosystem accelerating capability;
- Continue funding of a breadth of cyber-physical research;
- Invest in digital twins for transport; and
- Continue the delivery of the National Digital Twin Programme.[117]

Unlike the VR/AR Coalitions' Strategic Paper, the Consultative Response Paper provides concrete details for how the U.K. government should tackle cybersecurity challenges. The paper lists "high-level principles" that include (1) security as an enabler or ensuring systems or resilient; (2) secure-by-design; (3) necessity or understanding and mitigating risks and threats through necessary security controls; (4) a systems approach to security; and (5) learning from existing best practices.[118]

With the report just published in May 2023, it is still too soon to tell whether this report will sit on a shelf or if the government will use it as a bedrock to manage XR issues.

South Korea and Japan

Other countries such as South Korea and Japan are going full steam ahead with their XR ambitions and investing millions to accelerate the adoption rate among their citizens.

South Korea unveiled a $44.6 billion "Digital New Deal" to embrace new technologies, including XR technologies. This financial package includes over $170 million to help South Korea become the fifth most "metaverse-adopted county" by 2026, up from its current 12th-place status.[119] The government is investing this money in various metaverse projects to create a "metropolitan level metaverse platform" to provide government services.[120] For example, the city of Seoul created a "virtual public administration platform" where roughly 3,000 residents have engaged with the beta version.[121] Beyond government services, South Korea is seeing how it can integrate XR technologies in all aspects of society. Kakao Entertainment is working with a gaming company to create a K-pop band that only exists in the metaverse.[122] Through these investments, South Korea's domestic metaverse could be worth over $300 billion by 2026.[123] With the country filing one out of every five metaverse patents since 2016, second only to the United States, they are advancing towards this goal at a rapid pace.[124]

Complementing this investment is the implementation of the Metaverse Industry Promotion Act. The new law creates a Metaverse Policy Deliberation Committee to discuss policies related to the metaverse and requires the Minister of Science and Information and Communication Technology to establish a basic plan for the metaverse every three years.[125] This law builds off the Ministry of Science and Information and Communications Technology non-binding guidelines on the metaverse, which includes the core values of "secure identity, safe experience, and sustainable prosperity."[126] Stemming from these values are eight principles that metaverse system developers and users should abide by: authenticity, autonomy, reciprocity, respect for privacy, fairness, personal information protection, inclusiveness, and responsibility for the future.[127] While South Korea has not indicated whether they will integrate these principles into regulation, they have taken some initial steps, such as developing "metaverse specific regulation amendments" to protect minors from sexual harassment.[128]

Japan is similarly organizing its government to take full advantage of XR technologies. In a speech in front of Japan's Parliament at the end of 2022, Prime Minister Fumio Kishida said that the country will invest in digital transformation, which will include metaverse services.[129] He went on to say that Japan will "suppor[t] the social implementation of digital technology" and will "promote efforts to expand the use of Web3 services that utilize the metaverse." The government is well positioned to act on this as the Ministry of Economy, Trade, and Industry established a Web 3.0 Policy Office.[130] Recognizing the scope and breadth of Web 3.0 technologies, such as XR, the Office includes departments

responsible for industrial finance, taxation, corporate system (vehicles), media and content, sports, fashion, and other related industries.[131]

China

China and the metaverse must be viewed through two prisms. The first is their willingness to exploit vulnerabilities in the XR ecosystem. The second is their global ambition to become a market leader in XR technologies. Both of these prisms will have significant implications for the United States.

The China Threat

With the eventual increase of XR technologies used across critical infrastructure sectors, the United States must be mindful of the threat posed by China. The reason is straightforward. The U.S. government currently views China as the greatest cybersecurity threat facing the nation. The Office of the Director's National Intelligence's (ODNI) 2023 Threat Assessment Report notes, "China probably currently represents the broadest, most active, and persistent cyber espionage threat to [the] U.S. Government and private-sector networks. China's cyber pursuits and its industry's export of related technologies increase the threats of aggressive cyber operations against the U.S. homeland, suppression of the free flow of information in cyberspace—such as U.S. web content—that Beijing views as threatening to the CCP's hold on power, and the expansion of technology-driven authoritarianism globally. If Beijing feared that a major conflict with the United States were imminent, it would almost certainly consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide."[132]

This is not an exaggeration. China has shown a blatant willingness to attack U.S. companies and critical infrastructure beyond traditional espionage purposes. In May 2023, Microsoft found that a Chinese state-sponsored actor compromised U.S. critical infrastructure for the purpose of "develop[ing]… capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises."[133] State-sponsored actors have also been known to launch ransomware attacks, steal information on COVID-19 vaccines during their development, and pilfer military intellectual proprietary information.[134] Chinese actors were spotted as early as 2011 in American gas pipeline infrastructure, a troubling situation given the devastating impact that a ransomware attack had on the Colonial Pipeline in May 2021.[135] Their actions can be reckless with no care of who it impacts. In 2021, Chinese state-sponsored actors infiltrated Microsoft's Exchange servers and installed "web shells" across thousands of victims, creating a backdoor for any malicious actor to exploit. Although there were specific targets, their actions expanded to one of "mass exploitation" and were "indiscriminate" to the point that at least 60,000 Microsoft Exchange server customers were impacted.[136]

Based on open-source reporting, cyber actors affiliated with the People's Republic of China (PRC) have not been targeting XR applications or launching cyber attacks on XR devices. Yet, given the intelligence community's assessment of China's willingness to launch cyber attacks against U.S. critical infrastructure and its track record, the United States must be mindful of how China could exploit this new vulnerability in critical infrastructure systems.

There's a Plan for That

Relative to other country case studies, China has the most robust metaverse plan backed by significant resources and government intent to be a global leader in this space. This could have perverse impacts on the United States, as ODNI has noted that China is the United States' "top threat to U.S. technological competitiveness."[137] They further detail in their recent unclassified threat assessment that "China is doubling down on efforts to boost indigenous innovation and to become self-sufficient. China uses access to its vast market and control over critical supply chains as tools to force foreign companies and to coerce foreign countries to allow the transfer of technologies and intellectual property."[138] The combination of the threat posed by China in cyberspace, their willingness to actively penetrate American critical infrastructure and steal sensitive company and government information, and their desire to dominate a technological ecosystem like the metaverse warrants policymakers' attention on how China could exploit the XR market for potentially malicious ends.

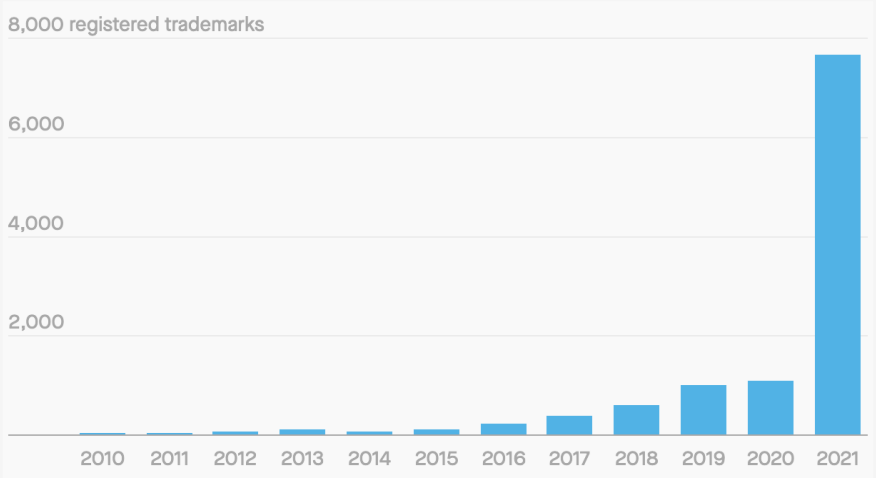
Similar to other segments of China's economy, the CCP has a plan for the metaverse. In November 2022, the Chinese Ministry of Industry and Information Technology released a five-year action plan solely dedicated to VR. The plan's goal, based on informal translations, is to "enhance the core technological innovation capabilities of the nation's virtual reality industry, stimulate the innovation vitality of the industrial service system, accelerate the integrated development of virtual reality and industry applications, and build and improve the innovation and development ecology of the virtual reality industry."[139]

The goal is for the Chinese industry to ship more than 25 million devices projected to yield nearly $50 billion in profits by 2026.[140] To achieve this, the PRC is investing in 100 "core" companies and forming 10 "public service platforms" by 2026.[141] The government also wants to achieve "breakthroughs" in various XR industries such as "industrial production, cultural tourism, integrated media, education and training, sports and health, business creativity, and smart cities."[142] One envisioned breakthrough is in education, where the plan details creating VR classrooms, teaching and research offices, and "laboratories and virtual simulation training bases" from primary schools through higher education. In health care, the PRC will promote XR in medical education, diagnosis and treatments, rehabilitation, addiction withdrawal assistance, therapy, and surgeries. They also intend to integrate XR into emergency services by hosting virtual drills for hazardous chemical safety and natural disaster prevention.[143]

China plans on launching 10 "virtual AR production application demonstrations," 10 "virtual reality+ integrated application pilot cities and parks," at least 20 "characteristic application scenarios," and 100 "pioneering cases of integrated applications."[144]

These are not just grandiose ideas. In 2021 alone, over 1,600 firms, including Alibaba and Tencent, applied for over 11,000 trademarks as shown in the graph below.[145] In that same year, more than $1.6 billion was invested in "metaverse-related ventures," and the China Mobile and Communications Association created the "Metaverse Industry Committee."[146] To underscore 2021 as a foundational year for the metaverse in China, the Metaverse Industry Committee released a book simply titled *Metaverse*, detailing the "rationale for the development of the next generation internet and the future digital economy."[147] The Committee appears to be one of the core implementers of the five-year action plan, as they will focus on drafting industry standards, creating industry roadmaps, and establishing an investor fund.[148]

Registered Trademarks in China Related to the Metaverse over Time



Source: Quartz, Qichacha

NEW AMERICA

In addition to breaking ground in various XR field applications, China wants to become a central leader in the supply chain. The five-year plan notes that China will "improve the supply capacity of the whole industry chain" by "comprehensively enhanc[ing] the industrialized supply capacity of key virtual reality devices, terminal peripherals, business operation platforms, content production tools, and dedicated information infrastructure." China also understands the importance of controlling the supply chain for the materials that

create VR headsets, as the plan details that they will "develop dedicated processing chips for VR, near-eye displays, and other key devices."[149]

Part of owning the supply chain is controlling the development of interoperability standards. Similar to how they were active in developing interoperability standards for global 5G devices, China has signaled they would like to lead in creating AR/VR standards.[150] China has made its desire to control the standards conversation clear, showing its confidence that the United States and other countries will be slow in reacting. The plan details that China will: "[B]uild a virtual reality comprehensive standards system covering the entire industry chain, including general use, content production, network transmission, distribution platforms, terminal equipment, quality evaluation, and innovative applications. We will clarify the roadmap for the development of virtual reality standards according to the urgent needs of the industry. We will accelerate the formulation and promotion of key standards such as health and comfort, user information security, content production process, transfer encoding, and employee capabilities. We will promote research on virtual reality application standards, and formulate model architecture and solution standards for different application scenarios. We will encourage Chinese enterprises and institutions to participate in international standardization activities and actively contribute to Chinese technical solutions."[151]

If China controls these standards it could jeopardize the safety, security, and privacy of any person or entity in the United States. For example, if China develops global manufacturing standards for user information security that is then embedded in systems widely used in the United States, those devices could have built-in vulnerabilities for the PRC to later exploit. Other possible standards could also make the transfer of data between systems insecure, less private, and more easily accessible to malicious actors. Further, if the standards are proposed in such a way that gives Chinese companies an upper-hand in the market, it could worsen the vulnerability landscape. Chinese companies are required, by law, to report to the Chinese government if they find a vulnerability in any of their products and cannot patch the vulnerability or to tell customers about it unless the government says so.[152] As a result, the PRC can sit on top of critical vulnerabilities and choose to exploit at their choosing.

If China can push forward with setting these global standards, the United States and its allies will eventually push back, which will further propagate the balkanization of the internet. A world could exist where there are Western XR standards and Chinese XR standards, and the devices that flow from those two realms would not be able to interoperate with each other. The Eurasia Group concluded similarly that there will be an increase in the decoupling of data flows, applications, and deeper layers of the tech stack, which "could lead to a Western democratic-centric decentralized metaverse(s) wholly or partially interoperable with more centralized, authoritarian, censored metaverse(s) running on largely Chinese hardware and embedded with the political preferences and social

controls coming from Beijing or Moscow."[153] The PRC also holds this sentiment, as an article in the *People's Liberation Army (PLA) Daily,* suggested that "[i]n the future, China and the United States will inevitably compete in the metaverse."[154]

However, the competition for the metaverse may only be hypothetical due to the United States' lack of involvement internationally. The United Nations International Telecommunications Union (ITU) has in recent years created a "Focus Group on the Metaverse." Through this working group, the UN is "analyzing the technical requirements of the metaverse to identify fundamental enabling technologies in areas from multimedia and network optimization to digital currencies, Internet of Things, digital twins, and environmental sustainability."[155] This represents a clear way for the United States to engage the international community on critical standards issues, yet the United States does not have a representative as a Vice-Chairman. In fact, the United States has no leadership positions or editorial representation in any of the 10 subworking groups, whereas China does.[156] In fact, the second ITU forum on "Creating a metaverse for all through international standards" was held in July 2023 in Shanghai. At this forum, key topics included the role of standards to build an open and interoperable metaverse, industrial metaverse, and the role of enabling technologies to unleash a new era of immersive and interactive experiences, all topics that China has a vested interest in.[157]

China's ambitions in the metaverse are not solely for economic reasons. National security concerns appear to be the primary driver. A Chinese think tank associated with the Ministry of State Security published a paper detailing three top concerns on how the metaverse could impact China's national security:

1. Other countries will develop XR technology faster than China, which could "cause instability in capability and access;"

2. The amount of sensitive data shared through XR will increase and the concern of how secure that data is could warrant the need to categorize XR technology as critical infrastructure; and

3. China's politics, economy, and society could be significantly altered by the metaverse, and therefore the Chinese Communist Party must pay great heed to how this technology is used.[158]

In addition to shoring up their national security, China also realizes that XR technology could be used for military purposes, similar to the United States. The government sees such close integration with XR and military applications that the *PLA Daily* news outlet created a term called the "battlefield metaverse" or "battleverse."[159] The *PLA Daily* has published several articles on the potential benefits of the battleverse, including performing training exercises in the battleverse, simulating war scenarios, testing new weapons, enabling research,

and supporting communications.[160] The battleverse could also allow soldiers stationed throughout China to have access to the same material and training opportunities regardless of location. The *PLA Daily* also warned how China's adversaries could use the battleverse to hurt China, and that it is, therefore, necessary for China to "develop the metaverse" so that they may "avoid wars and economic crises."[161]

These words have taken a life of their own as the PLA have begun integrating XR technology into their military procedures. For instance, the PLA created a VR parachute training system that "uses spatial positioning, virtual simulation, and other technologies to build a realistic parachute environment, allowing new paratroopers to perceive different aerial emergencies, thereby reducing risks in an actual parachute jump."[162] These simulations could also provide soldiers with experience in "unfamiliar environments...and improve their actual combat skills." The environment could be used to simulate joint operations and test prototype weapons.[163] Researchers from the Institute of Military Political Work, Academy of Military Sciences, a research institute within the PLA, also wrote an article entitled "The Metaverse: The New Heights of Future Cognitive Warfare," which details how cognitive warfare "can be advanced efficiently and enhanced at a fast pace" within the battleverse.[164] Based on open-source reporting, the PLA's use of XR technology pales in comparison to the U.S. military, yet the increased focus and attention on its military benefits will likely change that balance.

Regardless of how the PLA decides to integrate XR into their military services, China has thoroughly detailed how it intends to control large swathes of the XR supply chain, own the standards debate, and be seen as a leader in the metaverse. This, however, does not need to be a zero-sum game in which the United States and its allies try to crush China's burgeoning metaverse ambitions. A better tact would be to apply Secretary of State Antony Blinken's approach to China in which the United States "compete[s] with confidence...cooperate[s] wherever we can... contest[s] where we must."[165] The United States should support its own XR industries to successfully compete against state-sponsored Chinese companies to prevent China from completely dominating the supply chain or the XR ecosystem. The United States should welcome cooperation with China in the international arena, begin taking leadership positions in the ITU's Focus Group on the Metaverse, and convince China to adopt those standards within its territory. Finally, the U.S. government must be ready to contest the PLA's cyber activities and begin shaping international rules regarding how XR technology can and cannot be used for military purposes. This may also include examining XR apps that come from China with a critical eye for the data they may collect, similar to the national security concerns with TikTok and other Chinese apps. Other activities and policies will surely fall in these buckets, but the U.S. government must begin thinking about how to engage China in regards to XR, or else risks playing catch up and implementing haphazard policies.

The United States and the Metaverse

The United States government, in contrast to the EU, South Korea, and China, has largely ignored the rising cybersecurity implications of the metaverse and China's efforts to lead in this space. Admittedly, the U.S. government has issued several strategies on national security, emerging technology, and cybersecurity that could impact the security of XR technologies. The *2022 National Security Strategy* details that technology is "central to today's geopolitical competition and to the future of our national security," and highlights the importance of competing against China in the tech marketplace.[166] The *National Standards Strategy for Critical and Emerging Technology* also details the importance of the U.S. government working with private-sector partners and academia to lead in Standards Developing Organizations (SDOs) because the failure to do so could have security implications.[167] This point was also reiterated in the *2023 U.S. National Cybersecurity Strategy*, which calls for the need to engage in SDOs "to secure emerging technologies, enable interoperability, foster global market competition, and protect our national security and economic advantage."[168] The strategy also calls for securing supply chains, shifting liability for insecure software on the producers, and ensuring that holders of data are responsible stewards.

None of these strategies mention XR technologies as an emerging technology to keep an eye on.[169] Arguably, there will be some beneficial cybersecurity impacts on XR technologies if semiconductor supply chains are strengthened and if MSPs can secure the data they store. But without XR detailed in these national strategies, it is unlikely the U.S. government will devote time and resources to specifically address those unique challenges. The *National Cybersecurity Strategy's Implementation Plan*, for example, has thorough descriptions on how key parts of the strategy will be implemented, leaving little room—or resources—for deviation.[170]

Looking beyond these national strategies for XR-specific plans also shows that the United States is behind other countries. The Government Accountability Office and CRS have issued a few informational reports on metaverse focused on military applications and privacy concerns, but pass mentions of cybersecurity concerns.[171] NIST also has an "XR Community of Interest" that convenes subject matter experts whose work ranges from "visualizing crystalline structures to simulating public safety situations, performing usability testing, and creating standards," but their last "highlights post" was in 2021.[172]

In general, Congress as a whole has taken some steps, but nothing of significance. Congress was initially ahead of the game by creating the "Caucus on Virtual, Augmented, and Mixed Reality Technologies" in May of 2017 to "promote the advancing technologies of virtual reality, augmented reality, and

mixed reality to Members of Congress and their staff."[173] However, it is unclear what actions the caucus has taken since its inception. A handful of senators—unaffiliated with the Caucus—issued a letter to the Federal Trade Commission (FTC) on VR and children's privacy, and they urged the FTC to use authorities under the Children's Online Privacy Protection Act to protect children using VR devices.[174] In 2022, the House introduced a resolution to make November "National XR Month" to raise awareness of XR's economic impact. Specifically, the resolution noted that XR "plays an essential role in supporting United States national security objectives, where it is (1) used by the United States military for training programs; and (2) used for emergency preparedness and disaster response and management."[175] The resolution ultimately failed. Most recently, a bill was introduced in 2023 for the Labor Department to develop "immersive technology education and training programs for workforce development" that includes XR technologies, but it has not seen a vote in the House. Another bill would create a "Bureau of Digital Services Oversight and Safety" in the FTC to create regulations for a number of digital services, including AR and VR. And, apparently under the guise of Great Power Competition, one House member introduced a bill to "prohibit the use of Federal funds by the Department of Health and Human Services to award a grant for any virtual reality platform designed to teach children in China how to cross the street."[176]

Although these bills have failed to gain traction in Congress, some XR-related bills have become laws through the National Defense Authorization Act, including:

- Development of a digital health strategy by The Secretary of Defense to incorporate new and emerging technologies and methods, including virtual reality, in the provision of clinical care within the military health system;[177]
- Increased funding for airborne AR for pilot training; and[178]
- An analysis of whether emerging technologies, such as augmented reality, may aid in new shipbuilder training.[179]

Regardless of U.S. inaction, the combination of how the metaverse will impact society and other countries' policy responses to governing XR technologies illustrates that the metaverse is here and will continue to expand. XR technologies promise countless benefits, but the potential pervasiveness of the technology will introduce new vulnerabilities that malicious actors will surely exploit. While society will not collapse if a customer is unable to see how their kitchen would look like with sky blue walls, the incorporation and potential dependency of critical infrastructure and military actions on XR could pose a threat. Indeed, the United States saw a rise in ransomware attacks on schools and health care facilities when society transitioned their lives online with the onset of

COVID-19. It is therefore highly likely, if not expected, for malicious actors to find loopholes in hardware and software as XR devices and applications become increasingly popular. The impact could be alarming, ranging from compromised personal data to military espionage. It is time for the United States to take action.

Recommendations

Given the ubiquitous nature of XR technology, its increasing use in society, and geopolitical realities, the U.S. government and private-sector policymakers must take action. Policymakers should apply current cybersecurity best practices within XR technologies; learn from other countries by fostering innovation at home and examining the need for regulatory action; and engage with international partners on global norms and standards.

1. **Get on the same page.** The U.S. government desperately needs to coordinate how private-sector partners and academia will work together to securely incorporate XR technologies into our society. The U.K. and EU have established these exact forums and have already developed strategic documents and are iterating upon them, enabling them to fully embrace these technologies. The United States is woefully behind. The U.S. government should work closely with private-sector partners to determine what existing cybersecurity best practices—from security controls to frameworks to existing government policies—could apply to these technologies. Doing so will then help prioritize U.S. government and private-sector efforts to create new processes and security standards in those areas where existing best practices are not applicable. There will be a need for a strategic plan detailing a whole-of-society approach to XR in the near future, including government use of XR, securing XR technology, and cooperation and competition for the XR markets. A key part of this effort will be defining the "metaverse" to scope the effort and identify the relevant stakeholders.

2. **Encourage XR companies to adopt security frameworks and standards.** Companies involved in the XR ecosystem should adopt and implement existing cybersecurity frameworks. This could include the NIST Cybersecurity Framework, the Cybersecurity & Infrastructure Security Agency's (CISA) Cross-Sector Cybersecurity Performance Goals, or the Center for Internet Security's Critical Security Controls.[180] Adopting these standards does not necessarily mean their technologies will be secure, but it does improve their company's enterprise security, making it harder for malicious actors to gain access to their networks and infiltrate users' systems.

3. **Adopt stringent user authentication and zero trust authentication models.** With XR customers generating significant amounts of sensitive data, it will be imperative that strong log-in controls and access controls within XR companies and MSPs storing XR-generated data. Examples abound on how to strengthen user authentication from multi-factor

authentication, complicated passwords, and Fast Identity Online keys are models for strengthening user authentication, but companies should make these default settings rather than an opt-in service. While biometric logins have become increasingly popular, security practitioners should consider their appropriateness for logging into XR technologies. Additionally, XR companies and MSPs should implement zero trust authentication (ZTA) models into their systems to limit employee access to user data and other sensitive information. Employees have previously abused their unfettered access to user data, and ZTA can help prevent unauthorized access to that data.[181] Similarly, if an employee's account gets hacked, ZTA will make it difficult for a bad actor to access user and company data.

4. **Leverage secure by design, secure by default principles.** XR companies should look at CISA's Secure by Design, Secure by Default Principles to ensure that their products are built with security in mind and have security features that are easily accessible by the consumer.[182] Just as a car is secure by design due to airbags and automatic brakes and secure by default because of its seatbelts, XR technology providers must ensure that they are using proper memory safety code (secure by design) with multi-factor authentication enabled for logins (secure by default). This can also be extended to improving users' data privacy, in which XR platforms could detail in layman's terms the data it collects, how it is stored, for how long, and who has access to it.[183] The U.S. government should also work with the U.K., which included secure by design as a high-level principle in their Consultative Response Paper and signed onto CISA's principles, to further encourage companies to adopt these principles.[184]

5. **Get buggy with coordinated vulnerability disclosures and bug bounties.** The U.S. government should encourage security researchers to engage in U.S. government coordinated vulnerability disclosure (CVD) processes to safely and productively disclose vulnerabilities and coordinate mitigation efforts. Similarly, XR companies should adopt bug bounty programs to pay individuals if they find a vulnerability in their system. Meta, for example, has bug bounty programs for their Meta Quest controllers and pays up to $300,000 for certain vulnerabilities.[185] The combination of U.S. government and private-sector CVD programs will help security researchers find vulnerabilities formally and safely without fear of retaliation.

6. **Lead in developing international standards.** The U.S. government must work with its private-sector partners in the international community to develop security and other standards to counter China's efforts to lead international standards. The U.S. government must learn from its mistake

in 5G and proactively work with associations and companies to engage in international standards conversations, similar to the EU Commission's collaboration with the VR/AR Coalition. The Metaverse Standards Forum, for example, includes companies like Adobe, Qualcomm, Epic Games, Meta, and others and is exploring how Standards Developing Organizations could be leveraged to create interoperability standards. The U.S. government can also collaborate with the XR Association, which has companies such as Google, Microsoft, Sony, and others to collectively tackle XR issues. The U.S. government can work with these private companies and associations to engage in the UN's ITU Focus Group on the Metaverse, work to place U.S. members in leadership positions, and counter China's efforts in standards development.

7. **Copy a page from our European friends and examine regulation**. While Washington may be pilloried for discussing regulation, policymakers must assess what existing regulations apply to XR, which ones need to be modified, and the gaps in regulation that need to be filled with new regulatory laws. The European Council found that their "existing regulations don't cover XR technology and the lack of globally accepted standards further contribute to security and interoperability issues," and it is likely that the United States will have a similar discovery.[186] U.S. policymakers would be wise to not ignore regulation as a tool in their toolbox. This would also be consistent with the *2023 U.S. National Cybersecurity Strategy*, which states that "new authorities will be required to set regulations that can drive better cybersecurity practices at scale."[187]

8. **Copy a page from our Asian allies and examine financial incentives.** Similar to how South Korea and Japan are directly investing in their XR sectors, the U.S. government should build off the strategy described above to determine how existing grants could be used to build the U.S. XR ecosystem. This includes looking at grants within the Infrastructure Investment and Jobs Act, the CHIPS Act, and the Inflation Reduction Act to determine whether it would be appropriate to invest in XR technologies.

9. **(Finally) do something about privacy.** Any cyber incident, regardless of technology, has the potential to directly or indirectly compromise privacy. Realizing that Congress has failed for years to pass any meaningful legislation on data privacy, the sheer amount of sensitive information produced by XR will be greater and more sensitive than that previously generated by internet-enabled devices. This is a prime issue for the Reality Caucus to explore, and industry partners should examine reports published by the X Reality Safety Intelligence, the IEEE, and others that offer in-depth solutions to the privacy challenge.[188]

10. **Incorporate XR companies into the critical infrastructure ecosystem.** The U.S. government should consider including XR technologies in the IT critical infrastructure sector so that it could leverage certain critical infrastructure authorities, forums, and information sharing protocols to enhance cybersecurity efforts. The U.S. government currently recognizes 16 critical infrastructure sectors, including a sector solely dedicated to IT that presumably includes some XR players like Apple, Microsoft, and Meta. However, this may not include other companies focused solely on XR technologies. Including them in the IT sector or making an XR subsector will help the government to better engage these companies as a collective and enable these companies to have a unified voice to communicate with the government. This relationship would not be built overnight. One way to build trust is to facilitate information sharing between the government and industry. XR companies, for example, should be made aware and taught how they could lean on the information sharing protections detailed in the Cybersecurity Information Sharing Act of 2015. Additionally, XR companies could consider creating an information sharing analysis organization initially, and, if it became a subsector, an information sharing analysis center to facilitate that information sharing.

Conclusion

The continued expansion and adoption of 5G will bring with it unimaginable, wonderful XR capabilities that society should welcome. In 2008, 4G began entering our lives. It was unthinkable then that we would use a cell phone to get into a stranger's car, translate a menu in a different language in real-time, or FaceTime someone from across the world with no lag time. Just as the app ecosystem benefited from 4G capabilities, XR technologies will also ride the wave of the 5G revolution. Yet, this incredible technological advancement will bring with it significant national security concerns. Other countries, such as China, recognize the opportunity of XR technologies and are actively paving the way to embrace it, while shaping the environment to their advantage. The United States, on the other hand, is comically behind. This must change. The debate as to whether the metaverse will happen or not is a distraction. It is already here. The question should be whether the U.S. government can learn from its past mistakes and work to foster a vibrant and safe XR ecosystem.

Notes

1 Timothy Marler, Zara Fatima Abdurahaman, Benjamin Boudreaux, and Timothy R. Gulden, *The Metaverse and Homeland Security* (Santa Monica, CA: RAND Corporation, 2023), https://www.rand.org/pubs/perspectives/PEA2217-2.html.

2 Ling Zhu, *The Metaverse: Concepts and Issues for Congress* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/misc/R47224.pdf.

3 Ling Zhu, *The Metaverse: Concepts and Issues for Congress* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/misc/R47224.pdf.

4 Matthew Ball, *The Metaverse: And How It Will Revolutionize Everything* (New York, NY: Liveright Publishing Corporation, 2022), 29.

5 Numaan Huq, Roel Reyes, Philippe Lin, and Morton Swimmer, *Metaverse or Metaworse? Cybersecurity Threats Against the Internet of Experiences* (Dallas, TX: Trend Micro Research, 2022), http://documents.trendmicro.com/assets/white_papers/wp-metaverse-or-metaworse-cybersecurity-threats-against-the-internet-of-experiences.pdf.

6 Mitra Pooyandeh, Ki-Jin Han, and Insoo Sohn, "Cybersecurity in the AI-Based Metaverse: A Survey," *Applied Sciences* 12, no. 24 (December 18, 2022), https://doi.org/10.3390/app122412993.

7 Timothy Marler, Zara Fatima Abdurahaman, Benjamin Boudreaux, and Timothy R. Gulden, *The Metaverse and Homeland Security* (Santa Monica, CA: RAND Corporation, 2023), https://www.rand.org/pubs/perspectives/PEA2217-2.html.

8 Matthew Ball, *The Metaverse: And How It Will Revolutionize Everything* (New York, NY: Liveright Publishing Corporation, 2022), 29.

9 Timothy Marler, Zara Fatima Abdurahaman, Benjamin Boudreaux, and Timothy R. Gulden, *The Metaverse and Homeland Security* (Santa Monica, CA: RAND Corporation, 2023), https://www.rand.org/pubs/perspectives/PEA2217-2.html.

10 Ling Zhu, *The Metaverse: Concepts and Issues for Congress* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/misc/R47224.pdf; Kelley M. Sayler, *Military Applications of Extended Reality* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/natsec/IF12010.pdf.

11 National Institute of Standards and Technology, "Computer Security Resource Center Glossary," Accessed March 2023, https://csrc.nist.gov/glossary?index=A.

12 Georg Ritterbusch and Malte Teichmannand, "Defining the Metaverse: A Systematic Literature Review," *IEEE Access* 11 (2023), https://ieeexplore.ieee.org/document/10035386.

13 Numaan Huq, Roel Reyes, Philippe Lin, and Morton Swimmer, *Metaverse or Metaworse? Cybersecurity Threats Against the Internet of Experiences* (Dallas, TX: Trend Micro Research, 2022), http://documents.trendmicro.com/assets/white_papers/wp-metaverse-or-metaworse-cybersecurity-threats-against-the-internet-of-experiences.pdf.

14 Ling Zhu, *The Metaverse: Concepts and Issues for Congress* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/misc/R47224.pdf.

15 Department for Science, Innovation and Technology, "Enabling a National Cyber-Physical Infrastructure to Catalyse Innovation: Consultation Document," *GOV.UK*, March 2, 2022, https://www.gov.uk/government/consultations/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation-consultation-

document-accessible-webpage#annex-a--summarising-a-range-of-key-cyber-physical-infrastructure-elements.

16 Alexandros Vigkos, Davide Bevacqua, Luca Turturro, and Silvia Kuehl, *VR/AR Industrial Coalition* (Luxembourg: Publications Office of the European Union, 2022), https://op.europa.eu/en/publication-detail/-/publication/9aaef6fd-28db-11ed-8fa0-01aa75ed71a1.

17 Ling Zhu, *The Metaverse: Concepts and Issues for Congress* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/misc/R47224.pdf.

18 Alexandros Vigkos, Davide Bevacqua, Luca Turturro, and Silvia Kuehl, *VR/AR Industrial Coalition* (Luxembourg: Publications Office of the European Union, 2022), https://op.europa.eu/en/publication-detail/-/publication/9aaef6fd-28db-11ed-8fa0-01aa75ed71a1.

19 Jennifer Dohrman and Caitlin McArdle, "The Full Potential of a Military Metaverse," *War on the Rocks*, February 18, 2022, https://warontherocks.com/2022/02/the-full-potential-of-a-military-metaverse/.

20 Alexandros Vigkos, Davide Bevacqua, Luca Turturro, and Silvia Kuehl, *VR/AR Industrial Coalition* (Luxembourg: Publications Office of the European Union, 2022), https://op.europa.eu/en/publication-detail/-/publication/9aaef6fd-28db-11ed-8fa0-01aa75ed71a1.

21 Alexandros Vigkos, Davide Bevacqua, Luca Turturro, and Silvia Kuehl, *VR/AR Industrial Coalition* (Luxembourg: Publications Office of the European Union, 2022), https://op.europa.eu/en/publication-detail/-/publication/9aaef6fd-28db-11ed-8fa0-01aa75ed71a1.

22 McKinsey & Company, "Meet the Metaverse: Creating Real Value in a Virtual World," *New at McKinsey Blog*, June 15, 2022, https://www.mckinsey.com/about-us/new-at-mckinsey-blog/meet-the-metaverse-creating-real-value-in-a-virtual-world.

23 *Value Creation in the Metaverse: The Real Business of the Virtual World* (New York, NY: McKinsey & Company, 2022), https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf.

24 *Metaverse Report—Future Is Here: Global XR Industry Insight* (Shanghai: Deloitte China, 2019), https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/metaverse-whitepaper.html.

25 *Value Creation in the Metaverse: The Real Business of the Virtual World* (New York, NY: McKinsey & Company, June 2022), https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf.

26 Department for Science, Innovation and Technology, "Enabling a National Cyber-Physical Infrastructure to Catalyse Innovation: Consultation Document," *GOV.UK*, March 2, 2022, https://www.gov.uk/government/consultations/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation-consultation-document-accessible-webpage#annex-a--summarising-a-range-of-key-cyber-physical-infrastructure-elements.

27 Alexandros Vigkos, Davide Bevacqua, Luca Turturro, and Silvia Kuehl, *VR/AR Industrial Coalition* (Luxembourg: Publications Office of the European Union, 2022), https://op.europa.eu/en/publication-detail/-/publication/9aaef6fd-28db-11ed-8fa0-01aa75ed71a1.

28 Sara Qamar, Zahid Anwar, and Mehreen Afzal, "A Systematic Threat Analysis and Defense Strategies for the Metaverse and Extended Reality Systems," *Computers & Security* 128 (May 2023): 103127, https://doi.org/10.1016/j.cose.2023.103127.

29 "VR/AR Industrial Coalition: Statement to Support the European VR/AR Ecosystem," *European Commission*, September 14, 2022, https://digital-strategy.ec.europa.eu/en/news/vrar-industrial-coalition-statement-support-european-vrar-ecosystem.

30 "PwC China: Entering the Metaverse," *PricewaterhouseCoopers*, https://www.pwccn.com/en/industries/telecommunications-media-and-technology/metaverse.html.

31 Sara Atske, *The Metaverse in 2040* (Washington, DC: Pew Research Center, 2022), https://www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040/.

32 Ling Zhu, *The Metaverse: Concepts and Issues for Congress* (Washington, DC: Congressional Research Service: 2022), https://sgp.fas.org/crs/misc/R47224.pdf.

33 Baily Martin, "Privacy in a Programmed Platform: How the General Data Protection Regulation Applies to the Metaverse," *Harvard Journal of Law & Technology* 36, no. 1 (2022), https://jolt.law.harvard.edu/assets/articlePDFs/v36/Martin-Privacy-in-a-Programmed-Platform.pdf.

34 *Value Creation in the Metaverse: The Real Business of the Virtual World* (New York, NY: McKinsey & Company, June 2022), https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf.

35 *Value Creation in the Metaverse: The Real Business of the Virtual World* (New York, NY: McKinsey & Company, June 2022), https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf.

36 "Microsoft Mesh: Connect like never before," *Microsoft*, https://www.microsoft.com/en-us/mesh.

37 Stevan Silva, "Gorillaz turn the world into a stage with augmented reality," *Google AR & VR*, December 14, 2022, https://www.blog.google/products/google-ar-vr/gorillaz-maps-music-video/.

38 "Gorillaz Presents Skinny Ape," *Warner Music UK*, https://skinnyape.gorillaz.com/?ref=https%3A//t.co/fsrc6XzTQQ.

39 "The Tech Stack for the Metaverse," *Roblox Blog,* March 17, 2023, https://blog.roblox.com/2023/03/tech-stack-metaverse/.

40 Catherine Thorbecke, "What Metaverse? Meta Says Its Single Largest Investment Is Now in 'Advancing AI,'" *CNN*, March 15, 2023, https://www.cnn.com/2023/03/15/tech/meta-ai-investment-priority/index.html.

41 Jon Porter, "Disney Reportedly Eliminates Metaverse Division in First Round of Layoffs," *The Verge*, March 28, 2023, https://www.theverge.com/2023/3/28/23659691/disney-metaverse-job-cuts-eliminated.

42 Filip Krawanski, "How Many People Play Pokemon Go? Pokemon Go Player Count," *Dexerto*, July 2, 2023, https://www.dexerto.com/pokemon/how-many-people-play-pokemon-go-pokemon-go-player-count-2132719/.

43 Alexandros Vigkos, Davide Bevacqua, Luca Turturro, and Silvia Kuehl, *VR/AR Industrial Coalition* (Luxembourg: Publications Office of the European Union, 2022), https://op.europa.eu/en/publication-

detail/-/publication/9aaef6fd-28db-11ed-8fa0-01aa75ed71a1.

44 Georg Ritterbusch and Malte Teichmannand, "Defining the Metaverse: A Systematic Literature Review," *IEEE Access* 11 (2023) https://ieeexplore.ieee.org/document/10035386.

45 The Obama Administration, "Presidential Policy Directive—Critical Infrastructure Security and Resilience," *The White House Office of the Press Secretary*, February 12, 2023, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

46 *Critical Infrastructures Protection Act of 2001*, 42 U.S.C. 5195c(e).

47 Jordan Fues, "How Augmented and Virtual Reality Enhance the Water and Wastewater Industries," *Envirosight's Pipe Inspection Technology Blog*, June 8, 2023, https://blog.envirosight.com/how-augmented-and-virtual-reality-enhance-the-water-and-wastewater-industries.

48 "Augmented Reality/Virtual Reality (AR/VR) Technology in Flood Risk Management Applications," *ERDCWERX*, August 23, 2022, https://www.erdcwerx.org/augmented-reality-virtual-reality-ar-vr-technology-in-flood-risk-management-applications/.

49 "Virtual Reality and Augmented Reality Solutions for the Aviation Industry," *Aviation Pros*, April 22, 2021, https://www.aviationpros.com/gse/gse-technology/blog/21219689/tecknotrove-systems-virtual-reality-and-augmented-reality-solutions-for-the-aviation-industry.

50 Citi (@citi), "Citi HoloLens Holographic Workstation," YouTube video, June 14, 2016, https://www.youtube.com/watch?v=0NogltmewmQ.

51 Plant Vision, "Multispectral Augmentation," Accessed August 2023, https://www.plantvision.org/.

52 Alexandros Vigkos, Davide Bevacqua, Luca Turturro, and Silvia Kuehl, *VR/AR Industrial Coalition*, (Luxembourg: Publications Office of the European Union, 2022, https://op.europa.eu/en/publication-detail/-/publication/9aaef6fd-28db-11ed-8fa0-01aa75ed71a1.

53 Ian Wright, "Augmented Reality Applications in Nuclear Power Plants," *Deloitte United States*, May 4, 2017, https://www2.deloitte.com/us/en/pages/consulting/articles/augmented-reality-applications-in-nuclear-power-plants.html.

54 Michael Morozov, "Why Telecom Companies Should Use AR," *Jasoren*, November 23, 2018, https://jasoren.com/ar-in-telecommunication/.

55 Timothy Marler, Zara Fatima Abdurahaman, Benjamin Boudreaux, and Timothy R. Gulden, *The Metaverse and Homeland Security* (Santa Monica, CA: RAND Corporation, 2023), https://www.rand.org/pubs/perspectives/PEA2217-2.html.

56 Linda Malecaj, "Augmented Reality Revolutionizing Mining Industry," *VSight*, August 9, 2021, https://vsight.io/blog/augmented-reality-revolutionizing-mining-industry/.

57 Robin Goswami, "AR and VR Can Solve Many of Core Oil and Gas Challenges," *Infosys*, Accessed August 15, 2023, https://www.infosys.com/insights/industry-stories/ar-vr-in-oil-gas.html.

58 The Editors of Encyclopaedia Britannica, "Flight Simulator," *Encyclopedia Britannica*, July 20, 1998, https://www.britannica.com/technology/flight-simulator.

59 Josh Baughman, "Enter the Battleverse: China's Metaverse War," *Military Cyber Affairs* 5 no. 1 (2022), https://digitalcommons.usf.edu/mca/vol5/iss1/2.

60 Katie Lange, "Virtual, Augmented Reality Are Moving Warfighting Forward," *U.S. Department of Defense*, February 10, 2022, https://www.defense.gov/News/Inside-DOD/Blog/Article/2079205/virtual-augmented-reality-are-moving-warfighting-forward/.

61 Shaun Waterman, "Space Force's Innovation Chief Thinks Investment in the Metaverse Could Pay Off for the Military," *Air & Space Forces Magazine*, February 11, 2022, https://www.airandspaceforces.com/space-forces-innovation-chief-thinks-investment-in-the-metaverse-could-pay-off-for-the-military/.

62 Kelley M. Sayler, *Military Applications of Extended Reality* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/natsec/IF12010.pdf.

63 Kelley M. Sayler, *Military Applications of Extended Reality* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/natsec/IF12010.pdf.

64 Kelley M. Sayler, *Military Applications of Extended Reality* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/natsec/IF12010.pdf.

65 Lisa Daigle, "Army Goes Deep into VR/AR for Training and Combat," *Military Embedded Systems*, October 17, 2022, https://militaryembedded.com/radar-ew/sensors/army-goes-deep-into-vrar-for-training-and-combat.

66 Lisa Daigle, "Army Goes Deep into VR/AR for Training and Combat," *Military Embedded Systems*, October 17, 2022, https://militaryembedded.com/radar-ew/sensors/army-goes-deep-into-vrar-for-training-and-combat.

67 Lisa Daigle, "Army Goes Deep into VR/AR for Training and Combat," *Military Embedded Systems*, October 17, 2022, https://militaryembedded.com/radar-ew/sensors/army-goes-deep-into-vrar-for-training-and-combat.

68 Curtis Shinsato, "Virtual Squad Training Simulates Patrolling Techniques, Tasks," *U.S. Army*, June 21, 2010, https://www.army.mil/article/41203/virtual_squad_training_simulates_patrolling_techniques_tasks.

69 Will Knight, "The US Military Is Building Its Own Metaverse," *WIRED*, May 17, 2022, https://www.wired.com/story/military-metaverse/.

70 Diana Correll, "Navy's New 'Project Avenger' Flight Training Program Aims to Produce Stronger Aviators," *Navy Times*, May 26, 2021, https://www.navytimes.com/news/your-navy/2021/05/25/navys-new-project-avenger-flight-training-program-aims-to-produce-stronger-aviators/.

71 Kelley M. Sayler, *Military Applications of Extended Reality* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/natsec/IF12010.pdf.

72 Kelley M. Sayler, *Military Applications of Extended Reality* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/natsec/IF12010.pdf.

73 Lockheed Martin, "F-35 Electro Optical Targeting System (EOTS)," Accessed August 15, 2023, https://www.lockheedmartin.com/en-us/products/f-35-lightning-ii-eots.html.

74 Kelley M. Sayler, *Military Applications of Extended Reality* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/natsec/IF12010.pdf; Frederick Shear, "IVAS' Campaign of Learning Ensures Development, Production and Fielding Remain on Track," *U.S. Army,* March 14, 2023, https://www.army.mil/article/264773/ivas_campaign_of_learning_ensures_development_production_and_fielding_remain_on_track; Will Knight, "The US Military Is Building Its Own

Metaverse," *WIRED*, May 17, 2022, https://www.wired.com/story/military-metaverse/.

75 Michael Morozov, "Augmented Reality in Military: AR Can Enhance Warfare and Training," *Jasoren*, September 27, 2018, https://jasoren.com/augmented-reality-military/.

76 Michael Morozov, "Augmented Reality in Military: AR Can Enhance Warfare and Training," *Jasoren*, September 27, 2018, https://jasoren.com/augmented-reality-military/.

77 Kelley M. Sayler, *Military Applications of Extended Reality* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/natsec/IF12010.pdf.

78 Kelley M. Sayler, *Military Applications of Extended Reality* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/natsec/IF12010.pdf.

79 National Critical Functions (NCFs) are functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. More at https://www.cisa.gov/topics/risk-management/national-critical-functions.

80 *Technical Report: Wearable Enterprise AR Security-Risks and Management* (Milford, MA: Augmented Reality for Enterprise Alliance), https://thearea.org/area-resources/wearable-enterprise-ar-security-report/.

81 People's Republic of China, "Action Plan for the Integration and Development of Virtual Reality and Industrial Applications," *Ministry of Industry and Information Technology*, November 11, 2022, https://docs.google.com/document/d/1NeSAh2cay1PUCGhshk0BC0QAoD_mTGdG70aK8t3DtFg/mobilebasic.

82 *Technical Report: Wearable Enterprise AR Security-Risks and Management* (Milford, MA: Augmented Reality for Enterprise Alliance), https://thearea.org/area-resources/wearable-enterprise-ar-security-report/.

83 *Technical Report: Wearable Enterprise AR Security -Risks and Management* (Milford, MA: Augmented Reality for Enterprise Alliance), https://thearea.org/area-resources/wearable-enterprise-ar-security-report/.

84 Emily Everson Layden, "Rutgers Researchers Discover Security Vulnerabilities in Virtual Reality Headsets," *Rutgers Today*, February 10, 2022, https://www.rutgers.edu/news/rutgers-researchers-discover-security-vulnerabilities-virtual-reality-headsets.

85 Emily Everson Layden, "Rutgers Researchers Discover Security Vulnerabilities in Virtual Reality Headsets," *Rutgers Today*, February 10, 2022, https://www.rutgers.edu/news/rutgers-researchers-discover-security-vulnerabilities-virtual-reality-headsets.

86 "Hacking the Metaverse," *Louisiana State University*, November 8, 2022, https://www.lsu.edu/mediacenter/news/2022/11/virtualreality_safety_metaverse_cybersecurity_hacks.php.

87 "University of New Haven Researchers Discover Critical Vulnerabilities in Popular Virtual Reality Application," *University of New Haven*, February 19, 2019, https://www.newhaven.edu/news/releases/2019/discover-vulnerabilities-virtual-reality-app.php.

88 Martin Vondráček, Ibrahim Baggili, Peter Casey, and Mehdi Mekni, "Rise of the Metaverse's Immersive Virtual Reality Malware and the Man-in-the-Room Attack & Defenses," *Computers & Security* 127 (April 2023): 102923, https://doi.org/10.1016/j.cose.2022.102923.

89 Sara Qamar, Zahid Anwar, and Mehreen Afzal, "A Systematic Threat Analysis and Defense Strategies for the Metaverse and Extended Reality Systems," *Computers & Security* 128 (May 2023): 103127, https://doi.org/10.1016/j.cose.2023.103127.

90 Sara Qamar, Zahid Anwar, and Mehreen Afzal, "A Systematic Threat Analysis and Defense Strategies for the Metaverse and Extended Reality Systems," *Computers & Security* 128 (May 2023): 103127, https://doi.org/10.1016/j.cose.2023.103127.

91 Karthik Viswanathan and Abbas Yazdinejad, "Security Considerations for Virtual Reality Systems," *arXiv*, January 23, 2022, https://arxiv.org/pdf/2201.02563.pdf.

92 Sara Qamar, Zahid Anwar, and Mehreen Afzal, "A Systematic Threat Analysis and Defense Strategies for the Metaverse and Extended Reality Systems," *Computers & Security* 128 (May 2023): 103127, https://doi.org/10.1016/j.cose.2023.103127.

93 Numaan Huq, Roel Reyes, Philippe Lin, and Morton Swimmer, *Metaverse or Metaworse? Cybersecurity Threats Against the Internet of Experiences* (Dallas, TX: Trend Micro Research, 2022), http://documents.trendmicro.com/assets/white_papers/wp-metaverse-or-metaworse-cybersecurity-threats-against-the-internet-of-experiences.pdf.

94 Mitra Pooyandeh, Ki-Jin Han, and Insoo Sohn, "Cybersecurity in the AI-Based Metaverse: A Survey," *Applied Sciences* 12, no. 24 (December 18, 2022), https://doi.org/10.3390/app122412993.

95 Numaan Huq, Roel Reyes, Philippe Lin, and Morton Swimmer, *Metaverse or Metaworse? Cybersecurity Threats Against the Internet of Experiences* (Dallas, TX: Trend Micro Research, 2022), http://documents.trendmicro.com/assets/white_papers/wp-metaverse-or-metaworse-cybersecurity-threats-against-the-internet-of-experiences.pdf.

96 Karthik Viswanathan and Abbas Yazdinejad, "Security Considerations for Virtual Reality Systems," *arXiv*, January 23, 2022, https://arxiv.org/pdf/2201.02563.pdf.

97 "Hacking the Metaverse," *Louisiana State University*, November 8, 2022, https://www.lsu.edu/mediacenter/news/2022/11/virtualreality_safety_metaverse_cybersecurity_hacks.php.

98 Sara Qamar, Zahid Anwar, and Mehreen Afzal, "A Systematic Threat Analysis and Defense Strategies for the Metaverse and Extended Reality Systems," *Computers & Security* 128 (May 2023): 103127, https://doi.org/10.1016/j.cose.2023.103127.

99 "Pokemon Go Used by Armed Robbers to Lure Victims into Trap," *The Independent,* July 20, 2016, https://www.independent.co.uk/news/world/americas/pokemon-go-armed-robbers-lure-victims-game-trap-us-a7130431.html.

100 Mitra Pooyandeh, Ki-Jin Han, and Insoo Sohn, "Cybersecurity in the AI-Based Metaverse: A Survey," *Applied Sciences* 12, no. 24 (December 18, 2022), https://doi.org/10.3390/app122412993.

101 Mark McGill, *The IEEE Global Initiative on Ethics of Extended Reality (XR) Report: Extended Reality (XR) and the Erosion of Anonymity and Privacy* (Piscataway, NJ: IEEE Standards Association, 2021), https://standards.ieee.org/wp-content/uploads/import/governance/iccom/extended-reality-anonymity-privacy.pdf.

102 European Commission, *European Declaration on Digital Rights and Principles*, February 7, 2023, https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.

103 European Commission, *The Virtual and Augmented Reality Industrial Coalition,* September 22, 2022, https://digital-strategy.ec.europa.eu/en/policies/virtual-and-augmented-reality-coalition.

104 Alexandros Vigkos, Davide Bevacqua, Luca Turturro, and Silvia Kuehl, *VR/AR Industrial Coalition* (Luxembourg: Publications Office of the European Union, 2022), https://op.europa.eu/en/publication-detail/-/publication/9aaef6fd-28db-11ed-8fa0-01aa75ed71a1.

105 Alexandros Vigkos, Davide Bevacqua, Luca Turturro, and Silvia Kuehl, *VR/AR Industrial Coalition* (Luxembourg: Publications Office of the European Union, 2022), https://op.europa.eu/en/publication-detail/-/publication/9aaef6fd-28db-11ed-8fa0-01aa75ed71a1.

106 Alexandros Vigkos, Davide Bevacqua, Luca Turturro, and Silvia Kuehl, *VR/AR Industrial Coalition* (Luxembourg: Publications Office of the European Union, 2022), https://op.europa.eu/en/publication-detail/-/publication/9aaef6fd-28db-11ed-8fa0-01aa75ed71a1.

107 European Data Protection Supervisor, "Metaverse," Accessed August 15, 2023, https://edps.europa.eu/press-publications/publications/techsonar/metaverse_en.

108 "Data Privacy Concerns Will Be Amplified by the Metaverse," *Verdict,* January 20, 2023, https://www.verdict.co.uk/data-privacy-metaverse-challenge/.

109 Baily Martin, "Privacy in a Programmed Platform: How the General Data Protection Regulation Applies to the Metaverse," *Harvard Journal of Law & Technology* 36, no. 1 (2022), https://jolt.law.harvard.edu/assets/articlePDFs/v36/Martin-Privacy-in-a-Programmed-Platform.pdf.

110 Thierry Breton, "People, technologies & infrastructure—Europe's plan to thrive in the metaverse," *European Commission,* September 14, 2022, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_5525.

111 Thierry Breton, "People, technologies & infrastructure—Europe's plan to thrive in the metaverse," *European Commission,* September 14, 2022, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_5525.

112 David B. Hoppe, "EU To Launch Global Metaverse Regulation In 2023; Will The US Follow Suit?" *Gamma Law*, December 7, 2022, https://www.mondaq.com/unitedstates/antitrust-eu-competition-/1258480/eu-to-launch-global-metaverse-regulation-in-2023-will-the-us-follow-suit.

113 Department for Science, Innovation and Technology, "Enabling a National Cyber-Physical Infrastructure to Catalyse Innovation: Consultation Document," *GOV.UK*, March 2, 2022, https://www.gov.uk/government/consultations/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation-consultation-document-accessible-webpage#annex-a--summarising-a-range-of-key-cyber-physical-infrastructure-elements.

114 Department for Science, Innovation and Technology, "Enabling a National Cyber-Physical Infrastructure to Catalyse Innovation: Consultation Document," *GOV.UK*, March 2, 2022, https://www.gov.uk/government/consultations/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation-consultation-document-accessible-webpage#annex-a--summarising-a-range-of-key-cyber-physical-infrastructure-elements.

115 Department for Science, Innovation and Technology, "Enabling a National Cyber-Physical Infrastructure to Catalyse Innovation: Consultation Document," *GOV.UK*, March 2, 2022, https://www.gov.uk/government/consultations/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation-consultation-document-accessible-webpage#annex-a--summarising-a-range-of-key-cyber-physical-infrastructure-elements.

116 Department for Science, Innovation and Technology, "Enabling a National Cyber-Physical Infrastructure to Catalyse Innovation: Consultation Document," *GOV.UK*, March 2, 2022, https://www.gov.uk/government/consultations/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation-consultation-document-accessible-webpage#annex-a--summarising-a-range-of-key-cyber-physical-infrastructure-elements.

117 Department for Science, Innovation and Technology, "Enabling a National Cyber-Physical Infrastructure to Catalyse Innovation: Consultation Document," *GOV.UK*, March 2, 2022, https://www.gov.uk/government/consultations/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation-consultation-document-accessible-webpage#annex-a--summarising-a-range-of-key-cyber-physical-infrastructure-elements.

118 Department for Science, Innovation and Technology, "Enabling a National Cyber-Physical Infrastructure to Catalyse Innovation: Consultation Document," *GOV.UK*, March 2, 2022, https://www.gov.uk/government/consultations/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation-consultation-document-accessible-webpage#annex-a--summarising-a-range-of-key-cyber-physical-infrastructure-elements.

119 Andrew Fenton, "Inside South Korea's Wild Plan to Dominate the Metaverse," *Cointelegraph Magazine*, December 8, 2022, https://cointelegraph.com/magazine/inside-south-korea-wild-plan-dominate-metaverse/.

120 Prashant Jha, "South Korean Government Becomes an Early Investor in the Metaverse," *Cointelegraph Magazine*, June 2, 2022, https://cointelegraph.com/news/south-korean-government-becomes-an-early-investor-in-metaverse.

121 Andrew Fenton, "Inside South Korea's Wild Plan to Dominate the Metaverse," *Cointelegraph Magazine*, December 8, 2022, https://cointelegraph.com/magazine/inside-south-korea-wild-plan-dominate-metaverse/.

122 Jin Yu Young and Matt Stevens, "Can K-Pop Make the Metaverse Cool?" *New York Times*, January 29, 2023, https://www.nytimes.com/2023/01/29/business/metaverse-k-pop-south-korea.html.

123 Andrew Fenton, "Inside South Korea's Wild Plan to Dominate the Metaverse," *Cointelegraph Magazine*, December 8, 2022, https://cointelegraph.com/magazine/inside-south-korea-wild-plan-dominate-metaverse/.

124 Andrew Fenton, "Inside South Korea's Wild Plan to Dominate the Metaverse," *Cointelegraph Magazine*, December 8, 2022, https://cointelegraph.com/magazine/inside-south-korea-wild-plan-dominate-metaverse/.

125 Lee Ji-yong, "The Minister of Science and Technology establishes a metaverse plan every three years... Heo Eun-ah Initiated Industrial Promotion Act," *Maeil Business Newspaper*, September 1, 2022, https://www.mk.co.kr/news/politics/10442636.

126 Korea Herald Editorial, "Guidelines for metaverse," *Korea Herald*, November 30, 2022, https://www.koreaherald.com/view.php.

127 Korea Herald Editorial, "Guidelines for metaverse," *Korea Herald,* November 30, 2022, https://www.koreaherald.com/view.php.

128 Korea Herald Editorial, "Guidelines for metaverse," *Korea Herald,* November 30, 2022, https://www.koreaherald.com/view.php.

129 Tim Hornyak, "Armed with Anime Avatars, Japan Bids to Conquer the Metaverse," *Japan Times*, December 5, 2022, https://www.japantimes.co.jp/news/2022/12/05/business/tech/japan-metaverse-avatars/.

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

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

132 Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 6, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

133 Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 6, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf; "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," *Microsoft Threat Intelligence*, May 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

134 Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 6, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

135 Cybersecurity and Infrastructure Security Agency, "Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," July 21, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a.

136 Department of Justice, *21-0755 AUSA McIntyre Motion to Partially Unseal Search Warrant and Related Docs*, April 13, 2021, https://www.justice.gov/media/1136141/dl.

137 Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 6, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

138 Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 6, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

139 People's Republic of China, "Action Plan for the Integration and Development of Virtual Reality and Industrial Applications," *Ministry of Industry and Information Technology*, November 11, 2022, https://docs.google.com/document/d/1NeSAh2cay1PUCGhshk0BC0QAoD_mTGdG70aK8t3DtFg/mobilebasic.

140 Josh Ye, "China Aims to Ship 25 Million Virtual Reality Devices by 2026," *Reuters*, November 1, 2022, https://www.reuters.com/technology/china-aims-ship-25-million-virtual-reality-devices-by-2026-2022-11-01/.

141 Josh Ye, "China Aims to Ship 25 Million Virtual Reality Devices by 2026," *Reuters*, November 1, 2022, https://www.reuters.com/technology/china-aims-ship-25-million-virtual-reality-devices-by-2026-2022-11-01/.

142 People's Republic of China, "Action Plan for the Integration and Development of Virtual Reality and Industrial Applications," *Ministry of Industry and Information Technology*, November 11, 2022, https://docs.google.com/document/d/1NeSAh2cay1PUCGhshk0BC0QAoD_mTGdG70aK8t3DtFg/mobilebasic.

143 People's Republic of China, "Action Plan for the Integration and Development of Virtual Reality and Industrial Applications," *Ministry of Industry and Information Technology*, November 11, 2022, https://docs.google.com/document/d/1NeSAh2cay1PUCGhshk0BC0QAoD_mTGdG70aK8t3DtFg/mobilebasic.

144 People's Republic of China, "Action Plan for the Integration and Development of Virtual Reality and Industrial Applications," *Ministry of Industry and Information Technology*, November 11, 2022, https://docs.google.com/document/d/1NeSAh2cay1PUCGhshk0BC0QAoD_mTGdG70aK8t3DtFg/mobilebasic.

145 Mary Hui, "China Is Eyeing the Metaverse as the next Internet Battleground," *Quartz*, November 17, 2021, https://qz.com/2089316/china-sees-the-metaverse-as-the-next-internet-battleground; Eduardo Baptista, "Analysis: A Metaverse with Chinese Characteristics Is a Clean and Compliant Metaverse," *Reuters*, January 26, 2022, https://www.reuters.com/markets/funds/metaverse-with-chinese-characteristics-is-clean-compliant-metaverse-2022-01-25/; Josh Baughman, "Enter the Battleverse: China's Metaverse War," *Military Cyber Affairs* 5 no 1 (2022), https://digitalcommons.usf.edu/mca/vol5/iss1/2.

146 Eduardo Baptista, "Analysis: A Metaverse with Chinese Characteristics Is a Clean and Compliant Metaverse," *Reuters*, January 26, 2022, https://www.reuters.com/markets/funds/metaverse-with-chinese-characteristics-is-clean-compliant-metaverse-2022-01-25/; "China Creates Metaverse Industry Committee," *Opengov Asia,* March 2, 2022, https://opengovasia.com/china-creates-metaverse-industry-committee/.

147 "China Creates Metaverse Industry Committee," *Opengov Asia,* March 2, 2022, https://opengovasia.com/china-creates-metaverse-industry-committee/.

148 "China's State-Backed Metaverse Committee Aims to Help Industry Join the 'Racetrack of the Digital Economy," *South China Morning Post*, May 11, 2022, https://www.yahoo.com/video/chinas-state-backed-metaverse-committee-093000362.html.

149 People's Republic of China, "Action Plan for the Integration and Development of Virtual Reality and Industrial Applications," *Ministry of Industry and Information Technology*, November 11, 2022, https://docs.google.com/document/d/1NeSAh2cay1PUCGhshk0BC0QAoD_mTGdG70aK8t3DtFg/mobilebasic.

150 People's Republic of China, "Action Plan for the Integration and Development of Virtual Reality and Industrial Applications," *Ministry of Industry and Information Technology*, November 11, 2022, https://docs.google.com/document/d/1NeSAh2cay1PUCGhshk0BC0QAoD_mTGdG70aK8t3DtFg/mobilebasic.

151 People's Republic of China, "Action Plan for the Integration and Development of Virtual Reality and Industrial Applications," *Ministry of Industry and Information Technology*, November 11, 2022, https://docs.google.com/document/d/1NeSAh2cay1PUCGhshk0BC0QAoD_mTGdG70aK8t3DtFg/mobilebasic.

152 Andy Greenberg, "How China Demands Tech Firms Reveal Hackable Flaws in Their Products," *WIRED,* September 6, 2023, https://www.wired.com/story/china-vulnerability-disclosure-law/.

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

154 Josh Baughman, "Enter the Battleverse: China's Metaverse War," *Military Cyber Affairs* 5 no. 1 (2022), https://digitalcommons.usf.edu/mca/vol5/iss1/2.

155 United Nations International Telecommunications Union, "ITU-T Focus Group on

Metaverse (FG-MV)," Accessed August 15, 2023, https://www.itu.int/en/ITU-T/focusgroups/mv/Pages/default.aspx.

156 United Nations International Telecommunications Union, "FG-MV Workplan, structure and list of deliverables," Accessed August 15, 2023, https://www.itu.int/en/ITU-T/focusgroups/mv/Pages/default.aspx.

157 United Nations International Telecommunications Union, "2nd ITU Forum on 'Creating a metaverse for all through international standards,'" Accessed August 15, 2023, https://www.itu.int/en/ITU-T/focusgroups/mv/Pages/default.aspx.

158 Josh Baughman, "Enter the Battleverse: China's Metaverse War," *Military Cyber Affairs* 5 no. 1 (2022), https://digitalcommons.usf.edu/mca/vol5/iss1/2.

159 Josh Baughman, "Enter the Battleverse: China's Metaverse War," *Military Cyber Affairs* 5 no. 1 (2022), https://digitalcommons.usf.edu/mca/vol5/iss1/2.

160 Josh Baughman, "Enter the Battleverse: China's Metaverse War," *Military Cyber Affairs* 5 no. 1 (2022), https://digitalcommons.usf.edu/mca/vol5/iss1/2.

161 Josh Baughman, "Enter the Battleverse: China's Metaverse War," *Military Cyber Affairs* 5 no. 1 (2022), https://digitalcommons.usf.edu/mca/vol5/iss1/2.

162 Josh Baughman, "Enter the Battleverse: China's Metaverse War," *Military Cyber Affairs* 5 no. 1 (2022), https://digitalcommons.usf.edu/mca/vol5/iss1/2.

163 Josh Baughman, "Enter the Battleverse: China's Metaverse War," *Military Cyber Affairs* 5 no. 1 (2022), https://digitalcommons.usf.edu/mca/vol5/iss1/2.

164 Josh Baughman, "Enter the Battleverse: China's Metaverse War," *Military Cyber Affairs* 5 no. 1 (2022), https://digitalcommons.usf.edu/mca/vol5/iss1/2.

165 Antony Blinken, "The Administration's Approach to the People's Republic of China," Transcript of speech delivered at The George Washington University, Washington, DC, May 26, 2022, https://www.state.gov/the-administrations-approach-to-the-peoples-republic-of-china/.

166 Biden-Harris Administration, *National Security Strategy* (Washington, DC: The White House, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf.

167 Biden-Harris Administration, *United States Government National Standard Strategy for Critical and Emerging Technology* (Washington, DC: The White House, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf.

168 Biden-Harris Administration, *National Cybersecurity Strategy* (Washington, DC: The White House, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

169 The National Security Strategy, for example, calls out microelectronics, advanced computing and quantum technologies, artificial intelligence, biotechnology and biomanufacturing, advanced telecommunications, and clean energy technologies.

170 Biden-Harris Administration, *National Cybersecurity Strategy Implementation Plan* (Washington, DC: The White House, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

171 *Science & Tech Spotlight: Extended Reality Technologie*s (Washington, DC: U.S. Government Accountability Office, 2022), https://www.gao.gov/products/gao-22-105541; Ling Zhu, *The Metaverse: Concepts and Issues for Congress* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/misc/R47224.pdf.

172 "Extended Reality," *NIST,* December 16, 2019, https://www.nist.gov/information-technology/extended-reality.

173 Suzan DelBene, "Reps. DelBene, Clarke, Flores, Issa and Lieu Form Reality Caucus," *U.S. House of Representatives*, May 3, 2017, https://delbene.house.gov/news/documentsingle.aspx?DocumentID=1953; Ling Zhu, *The Metaverse: Concepts and Issues for Congress* (Washington, DC: Congressional Research Service, 2022), https://sgp.fas.org/crs/misc/R47224.pdf.

174 Edward Markey, Kathy Castor, and Lori Trahan, "Letter to the FTC," *U.S. Senate*, February 16, 2022, https://www.markey.senate.gov/imo/media/doc/letter_to_ftc_-_vr_and_children.pdf.

175 U.S. Congress, H.Res.1399—Expressing support for the designation of the month of November 2022 as "National XR Month," September 28, 2022, https://www.congress.gov/bill/117th-congress/house-resolution/1399.

176 U.S. Congress, *H.R.6339,* July 11, 2018, https://www.congress.gov/bill/115th-congress/house-bill/6339/text.

177 U.S. Congress, *S.1605 - National Defense Authorization Act for Fiscal Year 2022*, December 27, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/1605/text.

178 U.S. Congress, *S.1605 - National Defense Authorization Act for Fiscal Year 2022*, December 27, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/1605/text.

179 U.S. Congress, *H.R.6395 - William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, January 1, 2021, https://www.congress.gov/bill/116th-congress/house-bill/6395/text.

180 "Cybersecurity Framework," *NIST*, November 12, 2013, https://www.nist.gov/cyberframework; "Cross-Sector Cybersecurity Performance Goals," *Cybersecurity and Infrastructure Security Agency,* Accessed August 15, 2023, https://www.cisa.gov/cross-sector-cybersecurity-performance-goals; "The 18 CIS Controls," *Center for Internet Security*, Accessed August 15, 2023, https://www.cisecurity.org/controls/cis-controls-list.

181 Rohan Goswami, "Meta Reportedly Disciplined or Fired More than Two Dozen Workers for Taking over Facebook User Accounts," *CNBC*, November 17, 2022, https://www.cnbc.com/2022/11/17/meta-disciplined-or-fired-employees-for-taking-over-user-accounts-wsj.html.

182 "Secure by Design," *Cybersecurity and Infrastructure Security Agency*, Accessed August 15, 2023, https://www.cisa.gov/securebydesign.

183 "The XRSI Privacy and Safety Framework," *X Reality Safety Intelligence,* September 8, 2020, https://xrsi.org/publication/the-xrsi-privacy-framework.

184 Department for Science, Innovation and Technology, "Enabling a National Cyber-Physical Infrastructure to Catalyse Innovation: Consultation Document," *GOV.UK*, March 2, 2022, https://www.gov.uk/government/consultations/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation-consultation-document-accessible-webpage#annex-a--summarising-a-range-of-key-cyber-physical-infrastructure-elements.

185 Danny Palmer, "Hacking the Metaverse: Why Meta Wants You to Find the Flaws in Its Newest Headsets," *ZDNET*, January 3, 2023, https://www.zdnet.com/article/hacking-the-metaverse-why-meta-wants-you-to-find-the-flaws-in-its-newest-headsets/.

186 Alexandros Vigkos, Davide Bevacqua, Luca Turturro, and Silvia Kuehl, *VR/AR Industrial Coalition* (Luxembourg: Publications Office of the European

Union, 2022), https://op.europa.eu/en/publication-detail/-/publication/9aaef6fd-28db-11ed-8fa0-01aa75ed71a1.

187 Biden-Harris Administration, *National Cyber Strategy* (Washington, DC: The White House, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

188 "The XRSI Privacy and Safety Framework," *X Reality Safety Intelligence*, September 8, 2020, https://xrsi.org/publication/the-xrsi-privacy-framework; Mark McGill, *The IEEE Global Initiative on Ethics of Extended Reality (XR) Report: Extended Reality (XR) and the Erosion of Anonymity and Privacy* (Piscataway, NJ: IEEE Standards Association, 2021), https://standards.ieee.org/wp-content/uploads/import/governance/iccom/extended-reality-anonymity-privacy.pdf.

NEW AMERICA