NATO Foundation
Defense College

Metaverse: Implications for Security and Intelligence

Fabio Vanorio

Ministerial Advisor, Italian Ministry of Foreign Affairs and International Cooperation

NATO Defense College Foundation Paper

The bottom line

The Metaverse is a new virtual dimension twinning physical and virtual subject seamlessly. The competition for these new virtual universes will radically change policymaking in the context of a "new digital world order" that will require a paradigm shift in cooperation and conflict, requiring fundamental choices. Who is out of this system, will become marginal in the very sphere of international relations. The Metaverse could be used by large institutions, corporations, and governments, to "regulate" social, political, and economic inequalities in already partially democratic societies, and to reduce the level of democracy where it exists by concentrating power in restricted governance groups. In addition to the need for technologically enlightened leaders, pluralistic access to these technologies will be necessary as the only way to ensure their responsible global development.

The Metaverse is a synthetic universe resulting from the convergence of virtually enhanced physical reality and physically persistent virtual space. There is no single unified entity called the Metaverse, rather there are multiple worlds that complement each other in which virtualization, tools and 3D web objects are incorporated into the physical environment.
In future, many of the Internet activities we now associate with the 2D Web will migrate into the 3D spaces of the Metaverse. This means that, with the development of Artificial Intelligence (AI)-based tools, we will be able to smartly blend 2D and 3D worlds to achieve the unique benefits of each integrated with the other.

According to Bloomberg, the size of the Metaverse market is expected to reach $800 billion by 2024 and about $2,5 trillion by 2030. The meta-universe, while not definable as a new "virtual economy," will contribute to the growth of manufacturing (where 3D environments offer ideal design spaces for rapid prototyping and decentralization of production spaces), logistics, and transportation (with AI offering virtual platforms for the development and testing of autonomous machine behaviours, to be transposed to the physical world).

While the metaverse is a digital mirror of the physical world, digital twins are the foundation upon which the metaverse will be built. The projected size by 2028 of the digital twin market has been estimated by Grand View Research to be $86 billion. The growth of the digital twin market is primarily driven by the Industry 4.0 and the associated quest for resource optimization and predictive

maintenance, the need for Industrial Internet of Things (IIoT) related solutions and the rise of smart building infrastructure aimed at efficient and sustainable energy consumption.

Dragging a digital twin into the metaverse allows us to completely recreate it with live data, but also to insert it into the rest of the rendered world (i.e., a very realistic artificial image from a computer-processed 3D model). This means that it will behave exactly as it does in the real world. An example is represented by evaluating the ability of a port authority to respond to a tsunami with moored ships, including oil tankers. This is possible in the metaverse through the use of real-time data, physical land assessment, digital twins of each object, and associated metadata.

Virtuality, which mixes physical and digital, characterizing the Metaverse is based on the convergence of Internet technologies and Extended Reality (XR). According to Milgram's Reality-Virtuality Continuum, XR integrates digital and physical in various degrees, ranging from augmented reality (AR), through mixed reality (MR) and ending in virtual reality (VR).

In AR, the user is in a real environment enriched by virtual data, but reality maintains a predominant role over the additional virtual data. In MR, the user moves through an environment where real and virtual data coexist. In VR, real data is completely replaced by virtual data. If AR aims to enrich reality with useful information for performing complex tasks, VR aims to replace the real world with a simulated one.

The use of AR/VR technologies can have serious national security implications.

Adversarial actors may take advantage of the reality-altering capabilities of these technologies without adequate security. Similar concerns arise from digital replication capabilities such as deepfakes, i.e., doctored images or videos featuring people performing actions that never occurred in reality. For example, digital alterations could make a person appear to be in a place where they are not or distort information military personnel receive on the ground during a crisis.

The metaverse makes the operational environment completely locked into virtuality. This does not mean that it should be considered harmless. What happens in "those" worlds, being unconditioned

by the constraints and limitations of the external world, opens up unimaginable creativity that could become even greater when coupled with machines that learn and think independently.

After September 11, 2001, cyberspace has often been seen negatively. This attitude did not apply to gaming whose environments were deemed by intelligence agencies to be useful for HUMINT and SIGINT research. As early as 2008, the U.S. Office of the Director of National Intelligence (ODNI) was conducting predictive analysis programs (so-called Foresight) including the "Reynard Project", at first applied to social dynamics in large-scale online gaming and shifted over time towards the behaviour analysis in multiplayer video games, focusing on users' behaviour in virtual worlds linked to the real world, based on their avatars, communication, and group dynamics.

The "Reynard Project" represented the first case of intelligence agency scrutiny of the correlation between avatars and real-world behaviour in multiplayer video games. After fifteen years, Meta (formerly Facebook) is maintaining correspondence with the military in conducting its research in the Metaverse.

Meta has recently acquired synthetic data start-up AI.Reverie and consolidated it into its Reality Labs division dedicated to building a shared virtual world. AI.Reverie was a contractor to the U.S. Air Force (USAF, under a three-year, $950 million services contract that was terminated "for convenience" in correspondence with the Meta acquisition) to develop an AI-based system for conflict management and improved command and control systems. Even with the termination of the aforementioned relationship with the Pentagon, the capitalized knowledge by AI.Reverie will accelerate Meta's capabilities to produce synthetic data to train machine learning algorithms to build metaverse types that will maintain a latent civil-military duality.

In fact, in 2020 AI.Reverie has concluded agreements to improve U.S. Army and Air Force intelligence collection, as well as to improve difficult terrain navigation capabilities using synthetic data for training. Specifically, AI's product would support the 7th Bomb Wing, part of the USAF command unit that conducts nuclear deterrence and global strike operations (Global Strike Command, Eighth Air Force).

Given the sensitivity of much of the research devoted to the Metaverse, serious concerns emerge as virtual environments become embedded in and connected to physical systems and networks. Hacking

actions could extract information about structures and systems, as virtual environments make use of data from digital twins of machinery and buildings.

In case of attacks on system operation, this reverberates on the integrity of the system, and since the virtual universe permanently stores information online, the overall cost of the damage suffered is greater than it would be in the current digital ecosystem. The theft of "avatar" assets and user information in synthetic worlds would also completely negate the value of the user, as well as damage to information storage systems, which would severely diminish the overall value of the virtual environment causing huge economic losses.

The highly immersive experience of the metaverse could also reverberate negatively on general behaviours. The virtual perceptions could "disconnect" users from real-world dynamics, creating behavioural anomalies back in real life. People's bodies will react to events in virtual reality as they would in the real world, with heartbeats speeding up in stressful situations. That same realism could also mean that harassment in the metaverse will be more visceral, intense and damaging; misinformation more vivid and more compelling; everyday experiences more fascinating and more engaging.

These security implications make it necessary to match the development of the Metaverse with necessary regulation. We can distinguish three levels. The lowest includes the Metaverse as actually experience, a space where there are objects, data, and content, dependent on the tools and platforms on which it is built. We will have many instances of the Metaverse, equally prolific as websites and blogging platforms, as tools become more ubiquitous. This in itself will force the Metaverse to be grouped into Multiverses, i.e., categories of Metaverse with similar classification or type (e.g., the Industry 4.0 Metaverse, the entertainment-based Multiverse, and so on). Doing so will determine a common set of standards, frameworks, and interoperability for groups of metaverses that will increase the sharing of content, data and user access modes. At the highest level, we will have the Omniverse, i.e., the set of Multiverse, marked by even more general interoperability standards among multiverses.

The competition at the heart of these new virtual universes will radically change policymaking in the context of a "new digital world order" that will require a paradigm shift in cooperation and conflict. The rise of the Metaverse will require political, military, economic, and social choices. If these

technologies become as common and relevant as we believe, those who choose not to participate will become marginal in the very sphere of international relations. The Metaverse could be used by large institutions, corporations, and governments, to "regulate" social, political, and economic inequalities in already partially democratic societies, and to reduce the level of democracy where it exists by concentrating power in restricted governance groups. In addition to the need for technologically enlightened leaders, pluralistic access to these technologies will be necessary as the only way to ensure their responsible global development.

Fabio Vanorio

He is a Ministerial Advisor serving in the Policy Planning Unit of the Public and Cultural Diplomacy Department of the Italian Ministry of Foreign Affairs and International Cooperation. An alumnus of Saint John's University in New York, his research in technology issues is carried out independently. The views in this paper are expressed in a personal capacity and are in no way attributable to the Italian Ministry of Foreign Affairs and International Cooperation.

Sources

Madhumita, Murgia. 2021. Facebook to build Metaverse with start-ups that had US military contracts. Financial Times.

Priestley, Theo. 2021. The Metaverse, the Multiverse, and the Omniverse. MetaPunk.

Schwirn, Martin. 2022. A legal minefield called the Metaverse. Computer Weekly.

Smart, E. John, Cascio, Jamais, and Paffendorf, Jerry. 2007. Metaverse Roadmap Overview. Pathways to the 3D Web.

Vanorio, Fabio. 2021. Metaverse and National Security. Internet 3.0 and the New Digital World Order. Observatory on Infoware and Emerging Technologies. Italian Institute for Strategic Studies "Niccolò Machiavelli", Rome.


NATO Foundation
Defense College