INTERPOL

INTERPOL TECHNOLOGY ASSESSMENT REPORT ON METAVERSE

October 2022

The Metaverse is considered to be **the next stage** in the development of the **Internet**. Powered by a broad range of technologies, including **virtual reality (VR), augmented reality (AR) and edge computing,** it aims to enable people around the world to access **shared 3D virtual environments.** Using an internet connection and specialized hardware like **VR headsets** or **haptic suits,** individuals can enter these virtual spaces via avatars, creating a sense of **"virtual presence".**

Despite being in its early stage, the emergence of Metaverse has the potential to be **a complete game changer** for societies across the world, including for **crime and law enforcement.** For instance, while it will enable us to interact in a far more immersive way, the Metaverse will inevitably **impact existing criminal threats** like crimes against children and fraud, and also **generate new forms of crime.** As such, the development of Metaverse will require proactive action by the global law enforcement community. INTERPOL is the focal point for the global law enforcement community, equipping police forces to not just effectively combat the misuse of Metaverse, but also harness its responsible use for a safer world.

CURRENT STATE OF THE METAVERSE AND POSSIBLE FUTURE DEVELOPMENTS

Many elements of the Metaverse already exist, with the gaming industry and content creators acting as key drivers. For instance, using virtual reality headsets like Meta's Oculus Rift and Google's Daydream, paired with a laptop, phone or gaming console, users can access a variety of online virtual worlds, such as **Meta's Horizon Worlds, Decentraland, OverTheReality, The Sandbox, Roblox** and **Minecraft.**

According to its proponents, in the near future the Metaverse will become **a pervasive part of everyday life,** with individuals using online 3D virtual spaces to **work, learn, share, seek entertainment** and **even access essential services like banking and healthcare** – similar to how individuals use smart phones to access the digital world today. Of course, this expansive vision for the future of the Metaverse, driven largely by large technology firms, is contingent on various technological advances, in fields like augmented reality, virtual reality, mixed reality (MR), edge computing, artificial intelligence (AI), 5G, blockchain, Non-Fungible Tokens (NFTs) and other decentralized applications.

Some of the emerging and possible future use cases of the Metaverse are listed below:

USE OF METAVERSE FOR CRIMINAL PURPOSES

The Metaverse will challenge police services to detect criminal activity and keep users safe from new kinds of crimes, coined 'metacrimes.' In fact, some law enforcement agencies have already received reports of crimes featuring the Metaverse, including fraud, online grooming of children, hacking, impersonation, stalking and sexual harassment. However, as the Metaverse grows in popularity, the list of crimes will only expand, in some cases defying imagination:

- Money laundering
- Data theft
- Child grooming and child sexual exploitation
- Harassment, sexual assault and stalking
- Cyberattacks in and from Metaverse
- Cyber-physical attack
- Financial fraud, social engineering and scams
- Counterfeiting and copyright infringements
- Terrorism recruitment and training
- The Darkverse

POLICY ISSUES AROUND METAVERSE

There are a number of policy issues connected to the Metaverse that will require international efforts to address. Some of the issues identified below are broader than just law enforcement, but they will have a major impact on policing:

Identity construct	Managing and establishing the authenticity of digital identities in the Metaverse will be a challenge for individuals and institutions, including law enforcement.
Secure-by-design, privacy, data protection, ethics and human rights	The volume of data collected by the firms operating the Metaverse will magnify the challenge to data protection, privacy, ethics and human rights, with implications for cross-border information exchange as well as building regulatory framework to ensure secure-by-design user experiences.
Navigating interoperability	Interoperatibility - the ability to unify economics, avatars and systems across different virtual worlds - is key to the concept of the Metaverse, but will likely present issues for industry leaders/consortiums and regulators.
Cybersecurity, content and conduct moderation, safety and health	Measures will have to be taken to ensure the safety of users online and offline. This could range from agreeing to certain technical standards to raising awareness about security risks, digital hygiene and «VR Hangover».
Bridging the digital divide, portability and accessibility	Since currently many parts of the world lack reliable broadband, hardware and/or digital skills needed to access the Metaverse, accessibility and inclusiveness are sure to emerge as key future issues.
Addressing legislative and regulatory gaps to enable criminalization	As law enforcement cannot police without legislation, there will be an urgent need for laws that criminalize acts that cause harm in or through the Metaverse. Such efforts may also include efforts to regulate the use and transactions of virtual assets, given their significant role in the Metaverse.

BUILDING LAW ENFORCEMENT CAPABILITIES ON METAVERSE

While policing the Metaverse will initially have a high cost for law enforcement, especially in terms of awareness raising, training, equipment and associated services, there is an opportunity to proactively prepare and contribute to shaping safer online environments. In line with INTERPOL's approach to new technologies, this section examines the Metaverse as a threat, tool and source of evidence.

a. Countering Metaverse Threats

Law enforcement needs to acquire the capacity to counter so-called "metacrimes." This will include:

- Raising awareness
- Developing a law enforcement presence
- Training officers
- Identity management
- Closing legislative gaps
- Threat analysis
- Intelligence sharing
- Investigative support
- Establishing partnerships

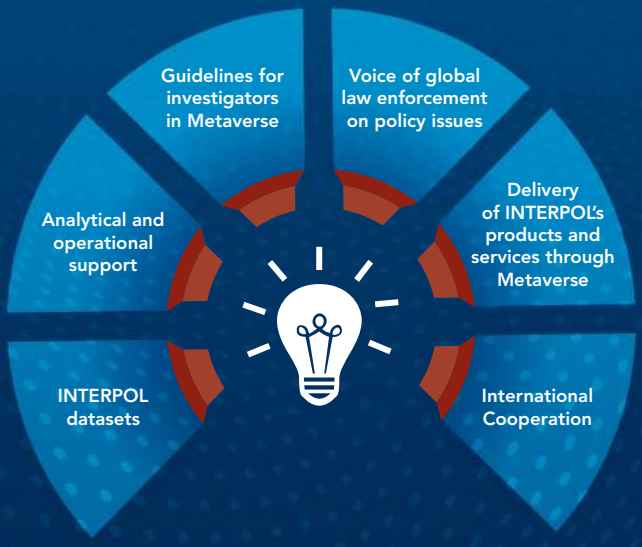
b. Using the Metaverse as a Tool

The rapid development of Metaverse related technologies brings not just threats but also opportunities for law enforcement agencies, provided that they can acquire the right skills, tools, and partnerships:

- Remote working
- Building partnership and networking
- Training and learning
- Digitalizing crime scenes

c. Forensics in the Metaverse

As people increasingly use the Metaverse to carry out all sorts of activities, including socializing, learning, working, and earning, it will emerge as a very important source of data and evidence for investigators.

- Accessing data from VR headsets and haptic devices
- Recovering evidence from the Metaverse infrastructure
- Getting data from the third party Metaverse service providers
- Training first responders, forensic specialists, and the entire criminal justice system

INTERPOL'S ROLE