Oct 2024

Reference Guide

Metaverse


Image created with DALL-E 3

Definitions

Metaverse: a network of interconnected two dimensional (2D) and three dimensional (3D) physical and digital worlds and environments of a (semi-) immersive nature that can be experienced with a sense of presence. *Source*

Augmented Reality (AR): a technology that superimposes a computer-generated image on a user's view of the real world, thus providing a composite view. *Source*

Virtual Reality (VR): the computer-generated simulation of a three-dimensional image or environment that can be interacted with in a seemingly real or physical way by a person using special electronic equipment, such as a helmet with a screen inside or gloves fitted with sensors. *Source*

Mixed Reality (MR): the blending of the physical world with the digital world. It allows the superposition and interaction between digital elements and the real-world environment to varying degrees. *Source*

Extended Reality (XR): the spectrum of virtual and augmented experiences, which merges the physical and virtual worlds to create engaging and immersive environments where users can interact with computer-generated elements in real-time. *Source*

Section.1 Metaverse in the News

The Metaverse and Its Dark Side: Confronting The Reality Of Virtual Rape

Forbes; January 16, 2024; ***Link to Article***

The police in the UK are currently investigating a virtual rape in the metaverse involving a young girl under the age of 16 who was sexually attacked by a gang of adult men in an immersive video game. That experience is alleged to have caused significant psychological trauma reminiscent of that experienced in a physical assault. This highlights a crucial aspect of virtual reality technologies: they are designed to be immersive, making experiences in the virtual world intensely real. The psychological impact of such virtual experiences cannot be underestimated, especially when they involve violent or traumatic events.

This is not the first report of sexual assaults in the metaverse. During the beta testing of Meta Horizon Worlds in November 2021, a user was virtually groped. In December 2021, a metaverse researcher's avatar was virtually raped by a group of male avatars who also harassed and photographed her. Another instance in May 2022 involved a SumOfUs researcher who was virtually raped in a private room by a user during a party, observed by others. These incidents highlight serious concerns about user safety and the effectiveness of existing protective measures in virtual reality environments.

Law Enforcement's New Frontier: Tackling Emerging Cybercrime in Virtual Worlds

Blockhead; January 20, 2024; ***Link to Article***

The Metaverse, a burgeoning digital frontier, is increasingly mirroring the complexities of the real world, including the prevalence of cybercrimes. A new white paper by Interpol has emphasized the urgent need for enhanced law enforcement in this virtual realm.

Dubbed "metacrimes," cybercrimes in the Metaverse range from grooming, radicalization and cyber-physical attacks against critical infrastructure, as well as theft of 3D virtual/ cultural property, trespassing in private virtual spaces, and robbery from an avatar. As the digital and physical worlds converge, these crimes have tangible consequences, demanding a novel approach to law enforcement, the cross-border law enforcement agency said in "Metaverse: A Law Enforcement Perspective."

Among the unique challenges the Metaverse presents for law enforcement, Interpol highlighted the lack of standardization and interoperability, issues of jurisdiction, user anonymity, and the intangible nature of digital evidence. "Police may be faced with virtual crime scenes where there is no physical evidence to be collected – just digital interactions involving virtual assets such as cryptocurrencies and non-fungible tokens (NFTs)," Interpol said.

Section.2 What is the Metaverse?

The Metaverse is a cloud distributed, multi-vendor, immersive-interactive operating environment that users can access through different categories of connected devices (both static and mobile).

It uses Web 2.0 and Web 3.0 technologies to provide an interactive layer on top of the existing internet.

It is an open platform for working and playing inside a VR/AR/MR/XR environment.

It will allow players to seamlessly move between virtual spaces together with their virtual assets.

The Metaverse is not merely a platform for human users; it will also be a communications layer for smart city devices through which humans and AI can share information.

Source: Trend Micro

Link to Metaverse Timeline

PAST

1992 The term "Metaverse" originated in Neal Stephenson's science fiction novel *Snow Crash.*

2003 Second Life, often described as the first Metaverse, incorporates social media aspects into a persistent 3D world where users are represented as avatars.

2017 Microsoft acquires AltspaceVR, integrating virtual avatars and meetings into Microsoft Teams.

2019 Facebook launches Facebook Horizon, a social VR world.

2021 Facebook (now Meta Platforms) commits to developing the Metaverse.

PRESENT

- The metaverse evolves with Web3 technologies, bridging virtual reality and digital experiences.
- Companies explore immersive possibilities, but challenges like privacy and user safety persist.
- Large enterprises like NVIDIA and Unity invest in foundational infrastructure.
- Platforms like Roblox, Decentraland, and Sandbox compete to be preferred portals.
- Web3 studios collaborate with leading brands to expand their market share.

FUTURE

Rapid Growth:

- Goldman Sachs projects that between 15% and 33% of global digital transactions will eventually shift to the Metaverse.
- Citigroup predicts that the Metaverse's market value will reach $8 trillion to $13 trillion by 2030.

Immersive Evolution:

- The Metaverse will grow exponentially, becoming more immersive and expansive.
- Expect more realistic avatars, enabling complex interactions in virtual worlds.

Section.3 Law Enforcement Considerations

BENEFITS

Next Level Capabilities

Metaverse technologies are transforming the landscape of law enforcement by introducing innovative AR, VR, and XR tools. Virtual reality solutions can provide immersive workspaces for law enforcement, and through 3D user interfaces, investigators will have a unique method for addressing intricate knowledge challenges. This technology is poised to be a game changing resource for police, and can reshape how law enforcement agencies navigate complex cases, delivering a fresh perspective and heightened clarity to investigations. *Interpol*

Advanced Training, Education and Simulation

Virtual reality can provide the type of training needed by today's law enforcement officers by allowing trainees to immerse their senses in a three-dimensional computer-generated environment. It allows for the training of rare and high stress situations that may be physically dangerous when experienced in the physical world and facilitate real-time collaboration, enabling police officers to coordinate and respond more effectively to different situations during daily operations. *Interpol; OJP; Europol*

Security of Critical Infrastructure

Contingency planning using the Metaverse can help ensure public safety and security, protect critical infrastructure, and facilitate disaster response. It can be used as a platform for simulating large-scale emergency situations, from natural disasters to chemical spills, and conducting rehearsals for responding to terrorist attacks. *Interpol*; *Rand*

Virtual Public Services and Reporting

Police departments and other government entities can establish a virtual presence in the Metaverse, offering services such as reporting crimes, filing complaints, or even hosting virtual community meetings. This virtual approach can make police services more accessible, particularly for those who may have mobility issues or for communities located in remote areas. *Interpol*

Crime Scene Preservation and Analysis

Law enforcement agencies can leverage the Metaverse to create virtual replicas of crime scenes, which can be accessed and analyzed long after the physical sites have been altered. *Interpol*

CHALLENGES

Law Enforcement and Digital Transformation

Law enforcement agencies will need to adapt and prepare for policing in the Metaverse. Though police have consistently adopted new technologies to improve public safety and operational efficiency, there will be an increased need for integrated and flexible digital capabilities to police the Metaverse. *Interpol*; *Europol*

Privacy and Surveillance

The Metaverse comes with concerns about data privacy. Law enforcement must navigate the ethical and legal implications of monitoring virtual spaces. *TechTarget*; *Interpol*

Jurisdictional Challenges

The Metaverse spans multiple geographies and jurisdictions, complicating law enforcement efforts due to uncertainties about applicable national laws. *SS8*; *IRPJ*

Limitations in Enforcement and Prosecution

Current legal protections are often ill-suited for the digital environment of the Metaverse. It may not be clear, for example, whether theft of metaverse assets constitutes a property crime. Legal authorities now have a crucial window to establish guidelines. Clear policies are needed to define what can be prosecuted, what data can be collected by lawful interception, and what is required from courts or other authorities to compel that collection. *SS8*; *McKinsey*

Image created with DALL-E 3

Section.4 Training in the Metaverse

Image created with DALL-E 3

Potential Benefits

1. Immersive Engagement
2. Global Accessibility
3. Personalized Training
4. Interactive Simulations
5. Collaborative Learning
6. Cost Efficiency

Articles and Resources

The Value of VR Training
Police Mag; April 5, 2024; Link to Article

The medium matters: Why virtual reality is breaking new ground in law enforcement training
Police1; February 5, 2024; Link to Article

Resources: *globalordnancenews*; *landvault.io*

Replicates High Stress Environments

Simulation training can replicate high-intensity situations like active shooter incidents and mass casualty events but in a safe environment where mistakes can be corrected. Training under manufactured stress helps build muscle memory and resiliency, honing officers' decision-making skills so the officer will be prepared mentally, physically and emotionally for real world scenarios.

Enhances De-escalation Training

Everyday police interactions that involve the need for complex de-escalation skills can be practiced within the Metaverse. Officers can enhance their communication skills in simulated environments with compliant and non-compliant individuals as well as mentally ill individuals and those suffering from addiction. Any scenario, whether dynamic or slow can be replicated.

Limitless Environments and Scenarios

As the Metaverse develops, environments and simulations will become limitless, allowing police officers to train in any simulated environment, including scenarios that would be difficult or impossible to replicate in real life like city centers, stadiums, airports, school buildings, or even certain law enforcement facilities. Thus, enhancing their ability to efficiently and safely respond to any location or incident.

Cost Effectiveness

VR training content is delivered digitally, eliminating costs associated with printed materials, manuals, and physical props. VR doesn't require dedicated physical spaces or expensive equipment and is scalable to each agency's budget. VR scenarios can be reused for multiple training sessions without additional costs. Updates and modifications are also easier to implement. Participants can engage in immersive learning experiences from anywhere, eliminating travel expenses.

Instructor Benefits

Real-time changes in scenarios can be made by the instructor to increase or decrease the difficulty and stress level. Instructors can receive regular progress reports and can keep track of the performance of the trainee. Most VR first responder training systems feature "see-what-I-see" functionality. This allows instructors to see what the trainee sees and experiences, allowing them to provide trainees with better post-training feedback or real-time guidance.

Unique Situations

When some officers experience a tragic or debilitating event on duty, whether it be an officer involved shooting or a emotionally traumatic event like a mass casualty incident or fatal incidents involving children, its sometimes challenging to help that officer get back to work and feel mentally and physically prepared. The Metaverse and VR can replicate challenging or significant scenarios for officers to revisit, helping them gain confidence to return to work.

Section.5 Crime in the Metaverse

Image created with DALL-E 3

The Metaverse has opened up opportunities for criminals to commit new types of crime, which can be referred to as "Metacrime". These crimes challenge traditional definitions of crime in the digital realm because they do not fit neatly into existing frameworks for reporting and investigating crime. Types of Metacrimes will only expand and challenge law enforcement to address emerging criminal activities. Metacrime is a growing concern and could become a major issue as the immersive world becomes part of our daily life.

NFTs

A non-fungible token (NFT) is a unique unit of data that is stored in a blockchain and can be sold and traded. NFTs regulate ownership of assets, but do not provide storage for the assets. This may lead to ransoming or other criminal attacks.

The Darkverse

The darkverse is like the dark web, except it exists inside the Metaverse. In some ways, it is more dangerous than the dark web because of the pseudo-physical presence of the users. It mimics clandestine physical meetings versus the purely online open discussion threads in dark web criminal forums.

Financial Fraud

Criminals will be drawn to the Metaverse because of the huge volume of e-commerce transactions that will occur in these worlds. There will be many who try and take advantage of users, steal their money, and capture their digital assets.

Privacy Issues

The Metaverse will likely be a collection of virtual worlds primarily created and hosted by big corporations, free to use for all interested persons. Metaverse publishers will control all aspects of their meta spaces, collect vast amounts of user data, and monetize the collected data.

Cyber-Physical Threats

The Metaverse is going to be an interactive application layer for the Spatial Web – a twinning of real and virtual realities enabled via billions of connected devices and accessed through VR/AR/MR/XR interfaces. This could give rise to cyber-physical threats. Critical infrastructure (CI) facilities will have physical equipment connected to digital twins.

Harassment and (Child) Abuse and Exploitation

Criminals may engage in virtual interactions with other users to commit assault or non-consensual and illicit offenses of sexual nature towards their avatars. This can range from instances of harassment to the creation and distribution of explicit sexual content. Children can be exploited to create games and virtual experiences to generate money. These malicious actors can put pressure on children to work more for more financial gain, which might not be given to them at the end. This can lead to abuse and child labor.

Social Engineering

The term "social engineering attacks" is used to describe a broad range of malicious activities accomplished through human interactions. Social engineering uses psychological manipulation to trick users into making security mistakes or give away sensitive information. *Source: WEF*

Bot and DDos Attacks

In Metaverse spaces, automated bots can impersonate legitimate users and take down entire virtual environments by overwhelming them with artificial digital traffic. Criminals can launch a DDoS attack to block access to virtual workspaces, shops, or event venues to commit a serious crime while the platform is down.

Terrorism

Terrorists may exploit the Metaverse for online recruitment, radicalization, training and indoctrination of individuals. They could also raise funds anonymously and easily spread disinformation and propaganda quickly reaching a global audience. Users engaging in cyberterrorism may lead to real world attacks with improved coordination and execution using a digital twin.

Sources: *Trend Micro; WEF; Responsible Metaverse Alliance; Police1; Europol; The Conversation; ncfaCanada*

Section.6 Articles - "Metacrime"

Money Laundering Threats To Metaverse

Financial Crime Academy; May 28, 2024; Financial Crime Academy

Due to the lack of laws and regulations around the trading of NFTs, the money laundering risk is considered high. Along with all the new opportunities, the Metaverse has some factors that invite criminals and money launderers to take advantage of the technology and system for their illegal advantages and gains. Identity theft, data hacks, breaches, and other financial crimes are all possible in the Metaverse as they are driven by the purpose of stealing personal information and accessing people's digital wallets for illicit activities. Big money can be moved here and there using the Metaverse due to the decentralized blockchain-based structure that links every task to digital wallets. Currently, there is no definitive idea of financial crime regulations applicable to the Metaverse. However, the lack of customer due diligence or CDD and Know Your Customer or KYC measures mean that users are generally less protected in the digital landscape. Inadequacy in terms of consensus and unified rules that apply to the Metaverse can become the reason that motivates criminals to pursue their illegal activities.

Police: Man uses Facebook's virtual reality platform to kidnap underage girl in real life

NBC24 News; March 11, 2022; nbc24.com

A teenage girl missing for several days was found by police in Cheyenne, Wyoming in the back of a semi-truck. For about a month, the teen and Evans had apparently been communicating via Oculus – Meta's (Facebook's) virtual reality platform. Just before leaving her home, investigators said she received an Oculus message saying, "I'm here." They said this was one of the first cases of its kind in the United States involving the Oculus system. Police were able to identify Evans in the case, and located him using cell phone data and communication apps. Within one hour of identifying Evans as the suspect, officers with the Cheyenne Police Department were able to locate the girl. Evans faces charges of kidnapping and harboring a runaway.

Cybercriminals target metaverse investors with phishing scams

CNBC; May 26, 2022; cnbc.com

A nurse in rural Maine. A fitness instructor in Colorado. A venture capitalist in Florida. All three invested in the Metaverse, buying land they say they thought was a solid investment. But in just days or months, all their virtual land was gone. And each of them says that there was simply no way to get it back. Investors across the country told CNBC that hackers stole their land in the Metaverse by tricking them into clicking on links they believed were genuine portals to the virtual universe, but which turned out to be phishing sites designed to steal user credentials. What they wanted was a piece of the Metaverse — a new, blockchain-based virtual set of platforms that has recently come to prominence because of significant involvement from celebrities, fashion shows and investors. Instead, they say they got a lesson in the dangers of high-risk investing.

Sexual Assault in the Metaverse: Virtual Reality, Real Trauma

Psychology Today; January 3, 2023; psychologytoday.com

The *New York Post* reported on the problem of sexual assault in the Metaverse, discussing how within Meta, the controversial rebrand of Facebook, women were reporting sexual abuse including everything from verbal to sexual abuse. London-based female researcher Nina Jane Patel shared her experience in her own words on Medium of being "verbally and sexually harassed" within 60 seconds of joining, by three to four male avatars, with male voices, who "virtually gang raped" her avatar and took photos, and when Patel tried to get away, they yelled "don't pretend you didn't love it" and other crude remarks. Virtual reality is designed to transport our brains into a virtual body, to trick us into experiencing an alternate existence in real-time. Accordingly, experiencing sexual assault or harassment online can create some of the same mental and emotional responses as in real life.

Image created with DALL-E 3

Section.7 Metaverse Resources and Reports

Resources

Virtual Reality (VR) Training Systems for First Responders Market Survey Report
DHS; January 2024; ***Link***

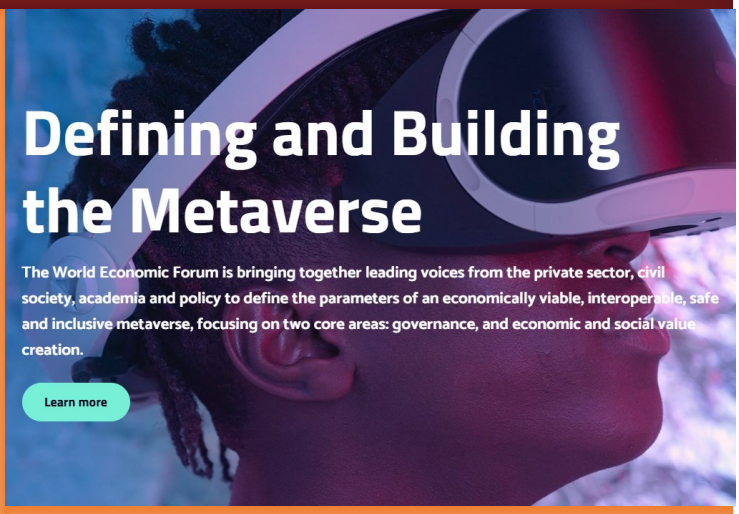
Metaverse Timeline
Jack X; ***Link***

Defining and Building the Metaverse
World Economic Forum; ***Link***

What is the Metaverse? An Explanation and In-Depth Guide
Tech Target; March 22, 2024; ***Link***

6 Global Companies Building up the Metaverse
Zebpay; September 28, 2023; ***Link***

What is the Metaverse? Step-by-Step Beginners Guide 2024
Blockchain Council; March 11, 2024; ***Link***



Reports

Interpol White Paper: Metaverse — A Law Enforcement Perspective
Interpol; January 2024; ***Link***

Metaverse Privacy and Safety
World Economic Forum; July 2023; ***Link***

Policing in the Metaverse: Prevention, Disruption, and Enforcement Challenges : Discussion Paper
Responsible Metaverse Alliance: June 2023; ***Link***

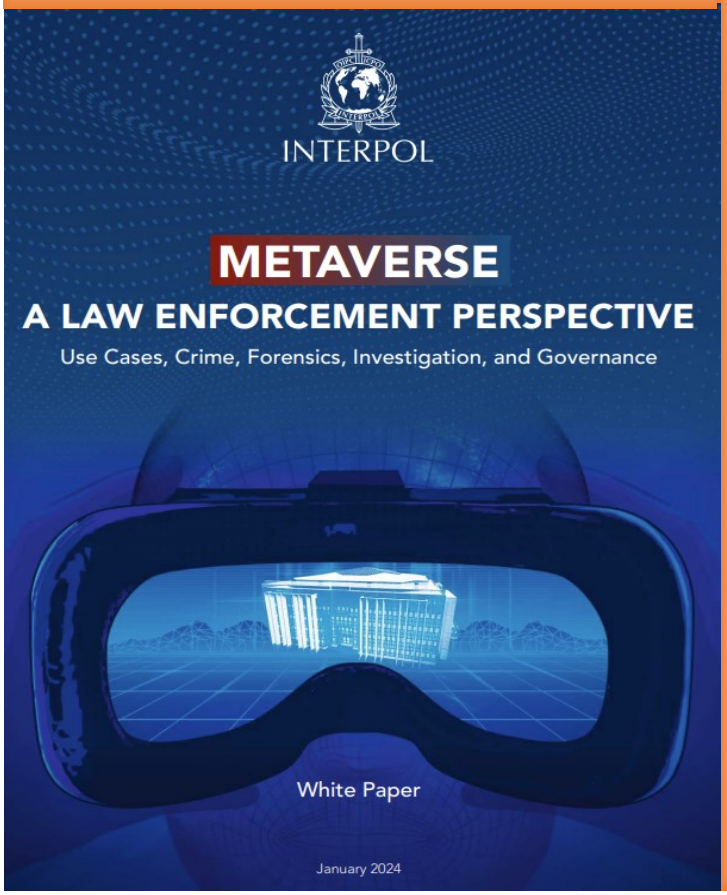
Policing in the Metaverse: What Law Enforcement Needs to Know
Europol; 2022; ***Link***

Metaverse or Metaworse? Cybersecurity Threats Against the Internet of Experiences
Trend Micro; 2022; ***Link***

The Metaverse and Homeland Security
RAND; May 2023; ***Link***

Interpol Technology Assessment Report on the Metaverse
Interpol; October 2022; ***Link***

Virtual Reality Training for Police Officers: a Comparison of Training Responses in VR and Real-Life Training
Police Practice and Research; Kleygrewe; January 30, 2022; ***Link***



Section.8 Key Takeaways

The Metaverse, a burgeoning digital frontier, is increasingly mirroring the complexities of the real world, including the prevalence of cybercrimes. (Section.1)

The Metaverse is a cloud distributed, multi-vendor, immersive-interactive operating environment that users can access through different categories of connected devices (both static and mobile). It uses Web 2.0 and Web 3.0 technologies to provide an interactive layer on top of the existing internet. (Section.2)

Law enforcement agencies have consistently adopted new technologies to improve public safety and operational efficiency. The digital transformation in policing now looks towards the extended reality and its materialization through the Metaverse as a prospective platform to further these aims. (Section.3)

Law enforcement agencies can benefit from training in the Metaverse due to the following: Immersive Engagement, Global Accessibility, Personalized Training, Interactive Simulations Collaborative Learning, Cost Efficiency. (Section.4)

The Metaverse has opened up opportunities for criminals to commit new types of crime, which can be referred to as “Metacrime”. (Section.5)

Within Meta, the controversial rebrand of Facebook, women were reporting sexual abuse including everything from verbal to sexual abuse. (Section.6)

Law Enforcement and private entities alike have produced numerous Metaverse reports and resources. (Section.7)

Questions can be directed to:

Monica Alnes Niklaus
Director of Projects
Major Cities Chiefs Association
monica@majorcitieschiefs.com