DOI: 10.53469/jssh.2024.6(08).02

Cybercrime in the Meta-Universe

Pallavi Lewandowsky

BBA LL. B 3rd Year, Bharati Vidyapeeth New Law College, Pune, Maharashtra, India

Abstract: ***The rapid evolution of technology has given rise to a virtual space called the Metaverse, where people interact, socialize and do business in an immersive digital environment. While virtual worlds have become an integral part of our daily lives, they have also become breeding grounds for all kinds of cybercrime. This research paper aims to explore the field of cybercrime in the virtual world and discover threats, challenges, and potential defenses. The study will also determine the motivation behind cyber crimes in the virtual world and examine the economic, social and political forces that drive the virtual world. Things are bad in these digital spaces. Understanding the motivation behind cybercrime in the virtual world is crucial to developing prevention and mitigation strategies. In this article, the current legal framework and regulations will be examined to solve the problems caused by cyber crimes in the virtual world and their suitability in the virtual environment will be evaluated. Additionally, solutions and best practices to increase security in the virtual world will be recommended to platform developers, users and law enforcement. At the end of this article, readers will have a better understanding of use the Metaverse and learn about potential strategies to combat these threats.***

Keywords: Metaverse, Extended Reality, Virtual world, Snow Crash, Blockchain

1. Introduction

Reality as we know it is undergoing historical change. Today's world is on the verge of a technological revolution that takes the "real world" we live in far beyond physical and time boundaries

Imagine a world where thousands of people live, work, shop, learn and interact with each other in the virtual world - all from the comfort of your couch in the physical world. In today's world, the computer screens we use to connect to the global information network have become doors opening to 3D virtual worlds at our fingertips; Just like real life, only bigger and better. This is called the Metaverse. Say goodbye to traditional offices. You may be surrounded by new interactive spaces and new spaces where you can make instant virtual connections with people, places, and businesses. Today's tools will allow you to connect and intuitively control 3D objects in the actual virtual environment you live in.

We believe that business has reached the cutting edge as technology evolves and integrates allowing us to enter a new virtual world. In this period of change, we need to connect augmented reality technology to the laws that govern it.

2. A Brief Overview of Metaverse

To understand the impact and legal implications associated with the Metaverse, let us first have a slight overview of the Metaverse and its associated history. Metaverse" became a household word when Facebook rebranded its corporate identity to Meta in October 2021 but it is far more diverse and giant. The word metaverse was first coined in the book 'Snow Crash' in year 1992. The story is set in a futuristic America and revolves around the Metaverse, a virtual reality space, and a cyber - drug called Snow Crash, which not only affects avatars in the digital world but also infects users in real life, leaving them in a vegetative state. [1]

To understand this clearly, we can isolate it from the internet. The Internet is a network of millions of computers, millions of servers and other electronic devices. Thanks to the Internet, Internet users can communicate with each other, view and interact with websites, and buy and sell goods and services. The Metaverse does not compete with the Internet; It is built on top of the Internet. The Internet is something people "see", but people can "live" in the virtual world to some extent. The development of the Internet has led to the emergence of many services that have led to the creation of the virtual world. The virtual world is what many in the industry believe is the vision of the next - generation Internet: a single, shared, integrated, continuous 3D virtual space where people can live in ways they cannot experience in the physical world. Some technologies, such as virtual reality (VR) headsets, augmented reality (AR) glasses, blockchain and Web3, provide access to this virtual world.

With an expected EUR 1.6 trillion boost to the global economy by 20305 and with 25% of people expected to spend at least an hour daily in the Metaverse6, it will certainly have an impact on the (in) security of citizens and be something law enforcement needs to be looking into. [2]

What should be considered a crime in Virtual World?

Before the Metaverse, there were MUDs (Multi - User Domains). MUD is a world of text without graphics. Users use commands to navigate various "rooms" and interact with others there. One of the most popular MUDs is LambdaMOO, its setting is based on a mansion in California. One night some users were chatting in the "living room". A user named Mr. Bungle suddenly used the "Voodoo Doll", a device that creates letters like John Kicks Bill to make it look like the user is performing the action. Mr. Bungle showed a user sexually assaulting and assaulting two people. Almost everyone agreed that Mr. Bungle did the wrong thing. How should we understand this error? People who think the virtual world is real will say that the experience is like reading a short story where you are attacked

The technology journalist Julian Dibbell reported a conversation with one of the victims recounting the assault:

Months later, the woman . . . would confide to me that as she wrote those words posttraumatic tears were streaming

down her face—a real - life fact that should suffice to prove that the words' emotional content was no mere fiction. [3]

The victim's experience lends support to the view that virtual reality is genuine reality, and that what happens in virtual worlds can be as meaningful as what happens in the physical world. All this raises crucial issues about the ethics of near - term virtual worlds. How should users act in a virtual world? What's the difference between right and wrong in such a space? And what does justice look like in these society.

Another similar recent incident that has happened in UK is the virtual gang rape of 16 year. The girl was reportedly wearing a virtual reality headset and playing an immersive game in the metaverse when her avatar was attacked by several others. There is an emotional and psychological impact on the victim that is longer - term than any physical injuries. [4]

Law enforcement and policymakers are asked to consider and prepare for the problems caused by crimes in the virtual world, because they will have real consequences for real people. As the virtual world continues to evolve, flexible and effective measures need to be developed to combat and prevent virtual crimes and ensure the safety of individuals in the field.

Adverse Use and Crimes in Metaverse

The occurrence of many types of crimes in the virtual world raises concerns about the need to identify and solve crime problems. Like blockchain mentioned above, new technologies will always provide criminals with new attackers. Criminals will have new opportunities to exploit these new technologies. Ransomware - type attacks can be particularly useful for Metaverse products. Given the importance of digital assets in the virtual world, accessing them can be particularly stressful. We will investigate how the virtual world will be used in some crime areas to provide a first - hand understanding of how the virtual world will impact the police.

Identity

As users' virtual representatives in the virtual world become more real and stable, there are concerns that fraud could be used to impersonate a person and steal their identity. Deep fakes are a type of electronic device that uses artificial intelligence to create real images, videos, or sounds that can be used to deceive others. Criminals can use deep learning technology to reliably reconstruct a user's face and steal a person's identity, causing trust issues and confusion in the support group. The integration of deep fakes into the Metaverse poses a major threat to security, especially in terms of fraud. This situation raises the issue of self - confidence of "people" in the virtual world; How can you determine who you are actually talking to?

Criminals have already been selling digital fingerprints on thedark web, which imitates the user's device's characteristics and behaviour. This allows a user of the service to use a browser plug into imitate a victim's digital fingerprint for the purposes of fooling authentication systems. [5]

With metaverse applications detecting unconscious signals, it may be able to present information to influence your decisions before you are even aware of it. Moreover, if the detailed personal information were used convincingly to imitate a person, this would make it very hard for law enforcement to know who the user is. The generation of very detailed biometric data may be inescapable, as it is required to provide the life - like immersive experience of the metaverse. The question will be how the platforms handle this kind of data, in what ways is it processed and stored, and what safeguards are implemented to prevent the harvesting of this information by third parties. It will remain to be seen how well the implementation of these platforms conform to the GDPR. [6]

Financial: Money Laundering, Scams

The more people learn about the Metaverse plans of big players like Epic Games and Meta, the more clear it becomes that maintaining anti - money laundering (AML) and know - your - customer (KYC) practices will be just as important internally. real world. In an environment populated by virtual businesses, selling virtual goods to avatars will require virtual profits. This provides the opportunity for money to be moved across borders in ways that are difficult for law enforcement to track. Cryptocurrencies are used for financial transactions and facilitate the transfer of criminal money. This number will increase with the further development and use of cryptocurrencies. The possibility of anonymous use of cryptocurrencies will make it difficult for the police to detect these crimes.

The world of NFTs is rife with frauds, as well as misappropriation of other people's assets. An NFT is a proof of ownership recorded on the blockchain and therefore unique and guaranteed to be so by the blockchain it is on. There are, however, ways to sell an NFT multiple times, using sufficiently different smart contracts or offering it on another blockchain. A seller does not even need to own what they offer to sell it as an NFT. While big marketplaces would presume to verify ownership, this is not practically possible because of the sheer number of NFTs being offered The result is a situation where as many as 80% of NFTs created with OpenSea's minting tool are estimated to be illegitimate [7]

Harrassment, Child Abuse and Exploitation

Harassment on the internet is already a significant issue, with as many as 58% of girls in an international 2020 Plan International survey having experienced online harassment. [8] Therefore, police should expect that this behavior also exists in the virtual world and may cause further harm to victims. The woman described the incident as rape. These virtual experiences raise serious questions about the validity of current policy. Exploitation requires physical contact, and avatars are virtual by definition. However, since the physical Internet is a way of describing the virtual world, it is obvious that with the development of technology, the distinction between physical and virtual will become even more problematic. As these experiences become more tangible and begin to feel real, we will need to decide when virtual experiences will have the same impact as physical experiences.

The current iteration of the Metaverse shows just how dangerous this can be for children. There is currently no (good) age rating for this site on Metaverse. On the VRChat social virtual reality platform, users experience strip clubs and children are exposed to dangers. Meanwhile, a sex "room" has been created on Roblox where people can talk about sex and their avatars can have virtual sex. . Platforms that provide these services must have a safe environment for children and protect the experience by monitoring content and behavior that violates their terms of use.

Terrorism

The virtual world offers terrorist groups new opportunities, especially in the areas of propaganda, recruitment and training. As the virtual environment becomes more realistic, criminals can better target and recruit vulnerable groups by tailoring their messages to specific biases. Additionally, VR can provide a useful environment for training, including the (re) creation of real situations. As digital twins of reality become more accurate, it will be possible to collect real - time information about the project, allowing future military personnel recruitment and planning to be done in the virtual world. The potential use of the virtual world by criminals has raised concerns from scientists and experts, highlighting the need to understand and address the security implications of these developments.

These virtual worlds can also allow them to impose strict rules on anyone who enters their “country”. This will create a truly equal world for these people and allow them to live in a situation contrary to generally accepted laws. Additionally, such a location would provide an excellent recruiting ground for other virtual worlds or even real - world crimes.

MIS and Disinformation

The current Web2.0 has given rise to the emergence of unprecedented precision in the capabilities to target specific demographics to influence their behaviour, whether it is for commercial or political gain. [9] On the old internet, it was possible to gather a lot of information about personal preferences and behavior to create travel plans by collecting data found on social media and tracking people's online behavior. This guide can be used to manage, identify and classify contacts online. More interaction provided by technology related to the virtual world will create a greater digital line. Unprecedented data will be collected, allowing for a better understanding and prediction of behavior and the ability to identify individuals based on specific interactions.

Understanding people's preferences and behavior not only provides more accurate information, but can adjust the content as well as the information plan based on this understanding.

What to do and what is being done?

1) Build Your Online Presence and Experience the Metaverse

Many countries have been investing in online policing, such as Estonia, Denmark, Norway, and Sweden. This is an important step to build valuable experience with virtual presence. Being present online makes police officers more approachable to people in remote locations and to people who spend most of their time online. With the great variety of available online platforms, it is important to gather experience on a few selected major platforms and build on the experience and tools acquired during this work.

Norway is a great example as it has started establishing its online presence in 2015 and now has ‘Nettpatrulje‘ or internet patrols in every district. This illustrates their advances with online policing. Moreover, Norway has been actively sharing their knowledge with other law enforcement agencies in Europe. [10]

France showed another example when it launched an initiative to establish a presence on Fortnite to be available for children suffering from abuse to share their stories. [11]

2) Analysis and Awareness of the Metaverse

New systems, such as the beginnings of the Internet, have been ignored by law enforcement in the past, with authorities even becoming acquainted with them in private.

New technology laws are often likened to driving with only a rearview mirror. This is usually done retroactively, when the new danger has come your way and it is too late. Therefore, predicting future damages is important to give the Department of Justice the opportunity to deal with potential problems. Officers must gain experience in the virtual world and find ways to introduce this special knowledge because they provide insights that can help understand what is going on and test innovation. We recommend that the police follow the development of the virtual world, the police start to gain experience online and the virtual world is renewed. Doing this will help organizations stay on track, evaluate progress, and intervene when problems arise.

Work with the Company that Created IT

Adapting a system to new regulations will be more difficult due to the regulations in the first place. Therefore, it is important that civil society and the police share the needs we put on the platforms in the early stages of Metaverse adoption. Therefore, active communication with the key people who make up the Metaverse platform is important because it allows both parties to understand each other better, help the platform remain secure, and help overcome the challenges of rules and governance. To meet the needs of law enforcement, a standard API may be needed to connect law enforcement to all platforms. These requirements should be determined at the beginning of the platform development process. Perhaps it could become part of the industry standard for Metaverse interaction, like the Metaverse Standards Forum.

1) Contractual Agreements

Establish clear terms of service and user agreements that outline acceptable behavior within the metaverse. Include provisions related to data protection, privacy, and consequences for engaging in cybercrimes.

2) Need of International Cooperation

Cybercrimes in the metaverse often transcend national borders. Encourage international cooperation and collaboration among law enforcement agencies to effectively address transnational cyber threats.

3) Public Private Partnerships

Foster collaboration between government agencies, private sector entities, and cybersecurity experts. Public - private partnerships can enhance information sharing and collective efforts to combat cybercrimes.

3. Conclusion

The Metaverse is still a long way from the vision presented to us by the people who created and invested in the Metaverse and other technologies. There is no way to know exactly what these developments will be, but technology is advancing rapidly. Each evolutionary step promises to make a real impact on people and law enforcement. The history of the Internet and other important technologies shows us that many unforeseen demands can arise. Ultimately, it is the unintended side effects of technology that will have the biggest impact. But to keep up with these developments, officials need to be out there and aware of technology. Understanding what is being created is crucial to ensuring the buy - in of all stakeholders and understanding the needs and responsibilities of policing in the virtual world. There is no doubt that it is a good thing to start building an online presence in the virtual world and gain experience using the tools available.

Online policing is a great way to learn what it means to be online and start building international networks. At the same time, investigative experience in areas such as blockchain and NFTs will provide valuable knowledge, information and skills to law enforcement.

For law enforcement to be successful in the investigation, special attention must be paid to the use of relevant technologies in online and virtual environments and continuous reporting efforts.

References

[1] NEEL STEPHENSON, SNOW CRASH 42, Bantam Books, New York, 1993

[2] Make Use Of, ‘These 8 Tech Giants Have Invested Big in The Metaverse’, 2022, [accessed 22 January 2024], https: //www.makeuseof. com/companies - investing - in - metaverse/

[3] http: //www.juliandibbell. com/articles/a - rape - in - cyberspace [accessed 24 January, 2024]

[4] https: //www.theguardian. com/commentisfree/2024/jan/05/metaverse - sexual - assault - vr - game - online - safety - meta [accessed 25 January, 2024]

[5] CreditUnionTimes, ‘The Rise of Digital Fingerprints in the Dark Marketplace Threatens Identities’, 2019, [accessed 25 January 2024], https: //www.cutimes. com/2019/08/28/the - rise - of - digital - fingerprints - in - the - dark - marketplace - threatens - identities/.

[6] Agencia Española de Protección de Datos, ‘Metaverse and Privacy’, 2022, [accessed 25 January 2024], https: //www.aepd. es/en/prensa - y - comunicacion/blog/metaverse - and - privacy

[7] Engadget, ‘Over 80 percent of NFTs minted for free on OpenSea are fake, plagiarized or spam’, 2022, [accessed 25 January 2024], https: //www.engadget. com/opensea - free - minting - tool - 220008042. html.

[8] PLAN International, ‘Online harassment is silencing girls: the EU and its Member States can do more and better’, 2020, [accessed 25 January 2024], https: //plan - international. org/eu/ blog/2020/11/25/online - harassment/.

[9] Bastick, Z., ‘Would you notice if fake news changed your behavior? An experiment on the unconscious effects of disinformation’, Computers in human behavior, Volume 116, March 2021, p.106633, [accessed 26 January 2024], https: //doi. org/10.1016/j. chb.2020.106633

[10] Politiet, ‘Police online patrols’, [accessed 26 January 2024], https: //www.politiet. no/en/rad/ trygg - nettbruk/police - online - patrol/

[11] Gadgets 360, ‘New Fortnite Mission: Reaching Out to Abused Children’, 2020, [accessed on 26 January 2024], https: //gadgets360. com/games/features/new - fortnite - mission- reaching - out - to - abused - children - 2247527