Chapter 1
Forecasting Cyber Crime in the Metaverse Era:
Future Criminal Methods – Readiness Requirements

Hossam Nabil Elshenraki
https://orcid.org/0000-0002-8131-5586
Dubai Police Academy, UAE

ABSTRACT

One of the digital transformation features of the new generation of cyber world is the meta verse. It is expected to establish a self-sustainable virtual ecosystem of fully immersive environments, real-time experiences with numerous chances to interact with the world for users and industrial businesses. With the introduction of new networks and enabling technological tools, the meta verse will succeed in the long term. However, with increasing interaction using new meta verse and a lot of third-party services, there would be an arena for many possibilities of cybercrime threats. Hence, combating cybercrimes is critical for the meta verse, and they should be investigated since the commercial adoption of the meta verse is imminent. Therefore, this chapter discusses many cybercrime methods and techniques which are expected in the meta verse environment, (AI) related cyber-attacks are expected, and solutions to the meta verse is possible.

INTRODUCTION: PROBLEM AND AIM OF THE BOOK EXPLAINED

Online users are exposed to many crimes such as online bullying, image-based abuse, such as sexual extortion, inciting children to sexual behaviour and exploitation, and given the high prevalence of interactive online games among children and youth.

Game environments can enable criminals to use avatars, disguising their real age and identity to target children. They can also provide a platform to post child pornography. In realistic scenarios generated by metaverse technology, children may not have yet developed critical thinking to help them identify risks.

DOI: 10.4018/979-8-3693-0220-0.ch001

Copyright © 2024, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

There were already concerns about online user safety, as it was found that more than 50% of girls had experienced online abuse.

Added to these online personal safety challenges are the risks to the police of personal data. Websites record the circulation of large amounts of data, including biometrics, location, and personal information.

This can provide new opportunities for criminals to commit identity theft, online fraud, and deception. Along with the growth of virtual currencies, which can provide unlimited space for criminals to defraud and steal users. (elliptic metaverse report, 2022)

BACKGROUND

Forecasting cybercrimes in the metaverse age is important because it is reflecting the need to proactively address emerging threats and safeguard the security and well-being of individuals within virtual environments, Forecasting helps in identifying potential cyber threats and criminal activities that may emerge within the metaverse, giving Early detection enables law enforcement and cybersecurity professionals to implement preventive measures before significant harm occurs, Understanding potential cybercrime trends allows for the development and implementation of proactive security measures, law enforcement can work collaboratively with technology providers to integrate security features and safeguards into virtual platforms, Forecasting assists law enforcement agencies in allocating resources efficiently based on anticipated cybercrime trends, prioritizing resources in areas with higher forecasted risks ensures a more targeted and effective response, Agencies can develop strategic plans for cybercrime prevention and response by aligning resources with forecasted threats, planning ahead helps in building specialized units, acquiring necessary technologies, and training personnel, it allows policymakers to anticipate changes needed in legal and regulatory frameworks to address emerging cyber threats, Timely updates to laws can provide a more robust legal foundation for prosecuting cybercriminals in the metaverse, that is why it is essential for adopting a proactive and strategic approach to cybersecurity, by anticipating and preparing for emerging threats, law enforcement, policymakers, and technology providers can collaboratively create a safer virtual environment for users and uphold the principles of security, privacy, and justice in the digital realm.

LITERATURE REVIEW

1- lik-hang lee, tristan braud, pengyuan zhou, lin wang, dianlei xu, zijun lin, abhishek kumar, carlos bermejo, and pan hui, fellow, ieee, all one needs to know about metaverse: a complete survey on technological singularity, virtual ecosystem, and research agenda, journal of latex class files, vol. 14, no. 8, September 2021 (Lik-Hang et al., 2021), the research study published in the Latex Class Files magazine, which is one of the magazines classified within the global Scopus index.

The study discussed the concept of mixed reality, and how the digital world will be from the perspectives of the ecosystem, which is meta verse world, with its new and completely different personalities, with what we live and see today.

The study concluded that with the involvement of emerging and progressive technologies to develop and improve ecosystems, and virtual world or digital twins may appear in another shape in the next years,

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/forecasting-cyber-crime-in-the-metaverse-era/334492

Related Content

Research on Digital Forensics Based on Uyghur Web Text Classification
Yasen Aizezi, Anwar Jamal, Ruxianguli Abudurexitiand Mutalipu Muming (2020). *Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice (pp. 485-496).*
www.irma-international.org/chapter/research-on-digital-forensics-based-on-uyghur-web-text-classification/252707

A Novel Pixel Merging-Based Lossless Recovery Algorithm for Basic Matrix VSS
Xin Liu, Shen Wang, Jianzhi Sangand Weizhe Zhang (2017). *International Journal of Digital Crime and Forensics (pp. 1-10).*
www.irma-international.org/article/a-novel-pixel-merging-based-lossless-recovery-algorithm-for-basic-matrix-vss/182460

Cyberterrorism: Can Terrorist Goals be Achieved Using the Internet?
Gráinne Kirwanand Andrew Power (2012). *The Psychology of Cyber Crime: Concepts and Principles (pp. 190-210).*
www.irma-international.org/chapter/cyberterrorism-can-terrorist-goals-achieved/60690

Investigations of Financial Fraud: Literature Analysis of Selected Financial Scams
Martynas Damulis (2023). *Theory and Practice of Illegitimate Finance (pp. 203-221).*
www.irma-international.org/chapter/investigations-of-financial-fraud/330633

Forensic Investigation of Peer-to-Peer Networks
Ricci S.C. Ieong, Pierre K.Y. Lai, K. P. Chow, Michael Y.K. Kwanand Frank Y.W. Law (2010). *Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions (pp. 355-378).*
www.irma-international.org/chapter/forensic-investigation-peer-peer-networks/39225