



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**TO BOLDLY GO WHERE NO METAVERSE HAS
GONE BEFORE: A VIRTUAL REALITY CHECK**

by

Madison K. Miller

September 2023

Co-Advisors:

Christopher Bellavita (contractor)
Mollie R. McGuire

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE September 2023	3. REPORT TYPE AND DATES COVERED Master's thesis		
4. TITLE AND SUBTITLE TO BOLDLY GO WHERE NO METAVERSE HAS GONE BEFORE: A VIRTUAL REALITY CHECK			5. FUNDING NUMBERS	
6. AUTHOR(S) Madison K. Miller				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) The metaverse may exert great power in virtual and real spaces and deliver significant economic and social benefits, but this power bears great risk of exploitation. This thesis explores security threats and implications for the homeland security enterprise with the widespread implementation of the metaverse. This thesis discusses the evolution of social media and online gaming, virtual reality, and the popularization of the metaverse. It reviews threats within the metaverse, including the transference of online criminal activity to the real world. A survey of user experiences in the metaverse demonstrates current security threats, including extremism, crimes against children, and financial crimes. Additional data from the Center for Countering Digital Hate validate these threats and the need to take preemptive action. The homeland security enterprise, emphasizing law enforcement and the intelligence community, should recognize the potential consequences of the metaverse and prepare for its mass-market success. This thesis recommends enhanced collaboration between industries to secure the metaverse against future threats.				
14. SUBJECT TERMS virtual reality, metaverse, Facebook, Meta, virtual worlds, immersion, security, surveillance, counterterrorism, cyber			15. NUMBER OF PAGES 109	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**TO BOLDLY GO WHERE NO METAVERSE HAS GONE BEFORE:
A VIRTUAL REALITY CHECK**

Madison K. Miller
Intelligence Analyst, Missouri State Highway Patrol
BS, Lincoln University, 2017
MS, Michigan State University, 2020

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2023**

Approved by: Christopher Bellavita
Co-Advisor

Mollie R. McGuire
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The metaverse may exert great power in virtual and real spaces and deliver significant economic and social benefits, but this power bears great risk of exploitation. This thesis explores security threats and implications for the homeland security enterprise with the widespread implementation of the metaverse. This thesis discusses the evolution of social media and online gaming, virtual reality, and the popularization of the metaverse. It reviews threats within the metaverse, including the transference of online criminal activity to the real world. A survey of user experiences in the metaverse demonstrates current security threats, including extremism, crimes against children, and financial crimes. Additional data from the Center for Countering Digital Hate validate these threats and the need to take preemptive action. The homeland security enterprise, emphasizing law enforcement and the intelligence community, should recognize the potential consequences of the metaverse and prepare for its mass-market success. This thesis recommends enhanced collaboration between industries to secure the metaverse against future threats.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	RESEARCH QUESTION	3
B.	LITERATURE REVIEW	3
C.	RESEARCH DESIGN	7
1.	Research Phases	8
2.	Institutional Review Board	8
II.	ONLINE GAMING AND SOCIAL MEDIA.....	9
A.	GAMING AS A SOCIAL PLATFORM.....	10
B.	CRIMINAL ACTIVITY IN SOCIAL MEDIA AND ONLINE GAMING	12
1.	Roblox	14
2.	Second Life	19
C.	CONCLUSION	22
III.	BACKGROUND OF VIRTUAL REALITY	23
A.	VIRTUAL REALITY ORIGINS AND CRITICAL TERMS.....	23
B.	PRE-OCULUS VR GAMING	28
C.	THE METAVERSE.....	30
IV.	CRIMINAL ACTIVITIES WITHIN THE METAVERSE	35
A.	CRIMES AGAINST CHILDREN.....	37
B.	FINANCIAL CRIMES.....	40
C.	TERRORISM.....	41
D.	CONCLUSION	43
V.	IMPLICATIONS FOR HOMELAND SECURITY	45
A.	DATA PRIVACY AND ENCRYPTION	45
B.	CONTENT MODERATION	47
C.	MONITORING AND SURVEILLANCE.....	48
D.	CIVIL LIBERTIES	48
E.	ANONYMITY	49
F.	DECENTRALIZATION	50
VI.	SURVEY	53

A.	METHODS	53
B.	SURVEY DATA.....	54
VII.	CENTER FOR COUNTERING DIGITAL HATE	57
VIII.	CONCLUSION	61
A.	FINDINGS	61
B.	RECOMMENDATIONS.....	62
1.	International Cooperation.....	63
2.	A Multi-disciplinary Approach	63
3.	Economics, Costs, and Regulation.....	64
4.	Potential Challenges.....	64
5.	Can't We Just Work Together?	66
C.	FUTURE RESEARCH.....	67
APPENDIX.	SURVEY QUESTIONS AND RESPONSES	69
LIST OF REFERENCES		77
INITIAL DISTRIBUTION LIST		89

LIST OF FIGURES

Figure 1.	Total Hours Streamed on Twitch.....	11
Figure 2.	Suspicious Activity Reporting Indicators and Behaviors.	17
Figure 3.	Sword of Damocles.....	23
Figure 4.	bHaptics VR Vest.	26
Figure 5.	bHaptics VR Vest Feedback Points.	27
Figure 6.	Omnifinity’s Omnideck VR Platform.....	27
Figure 7.	Beat Saber VR Game.	31
Figure 8.	Elite Dangerous VR Gameplay.....	32
Figure 9.	Projected Time Spent in the Metaverse by Generation in Five Years.....	33
Figure 10.	A Virtual Strip Club.....	39
Figure 11.	VR Gun Stock Accessories.....	42
Figure 12.	Metaverse Safety Concerns from 2022 Politico Poll.....	45
Figure 13.	Accounts of Assault by Metaverse Users	55
Figure 14.	Disturbing Reviews of VRChat in the Meta Store.....	60

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Immersive Haptic Devices for Use with Meta Quest Headsets.....	28
Table 2.	VR Headset Comparison.....	29
Table 3.	Content Violations Observed in VRChat by CCDH Researchers.	58

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AR	augmented reality
CCDH	Center for Countering Digital Hate
DAU	daily active user
IP	internet protocol
MTurk	Mechanical Turk
NPC	non-player controlled
NSPCC	National Society for the Prevention of Cruelty to Children
RMVE	racially motivated violent extremist
RP	role-playing
TOS	terms of service
VPN	virtual private network
VR	virtual reality

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The metaverse is a rapidly evolving technological innovation that may have a powerful impact on nearly every industry. The metaverse, owned by Meta (formerly Facebook), has been hailed as the “future of connection.”¹ As discussed in this thesis, the metaverse refers to Meta’s metaverse and the headsets used to access it, allowing users to access a massive open-world environment that hosts games, social communities, and even virtual workspaces.² Given its complex virtual environment, understanding the dangers in the metaverse better informs and prepares homeland security professionals and public safety to protect against threats as the platform gains momentum. This thesis underscores some of the major issues already present in the widespread commercial success of the metaverse and its affiliated technologies and emphasizes the need for better cross-industry collaboration and future research.

Contextualizing the significance of the metaverse for policymakers, this thesis traces the evolution of social media, online gaming, virtual reality (VR), and the subsequent commercialization of the metaverse. To illustrate the growing popularity of such spaces, Twitch—a streaming platform that hosts gamers in a live, interactive, video chatroom-style interface—saw record-breaking growth with three billion hours of consumer use in the first quarter of 2020 and five billion hours in the second quarter of 2020.³ A slew of factors complicates the intersection of crime and the internet. For as long as online gaming has existed, it has also facilitated illegal activity.⁴ Most communities exist for social good and cohesion, yet criminals exploit unique opportunities in online gaming. In many cases, the crimes

¹ “About the Metaverse,” Meta, accessed January 26, 2023, <https://about.meta.com/metaverse/>.

² “What Is the Metaverse?,” Meta, accessed January 26, 2023, <https://about.meta.com/what-is-the-metaverse/>.

³ Sarah Perez, “Twitch Breaks Records Again in Q2, Topping 5B Total Hours Watched,” TechCrunch, July 1, 2020, <https://techcrunch.com/2020/07/01/twitch-breaks-records-again-in-q2-topping-5b-total-hours-watched/>.

⁴ Kim-Kwang Raymond Choo and Russell G. Smith, “Criminal Exploitation of Online Systems by Organised Crime Groups,” *Asian Journal of Criminology* 3, no. 1 (June 2008), <https://doi.org/10.1007/s11417-007-9035-y>; Matthew S. Ruskin, “Playing in the Dark How Online Games Provide Shelter for Criminal Organizations in the Surveillance Age,” *Arizona Journal of International & Comparative Law* 31, no. 3 (2014), <http://arizonajournal.org/wp-content/uploads/2015/09/10-Ruskin.pdf>.

perpetuated online are financial or have a financial connection to the physical or natural world.⁵ Other examples include harassment, stalking, child exploitation, bullying, and revenge porn.⁶ Furthermore, researchers studying the most popular social app in Meta's VR app store have found that users, including minors, are exposed to abusive behavior once every seven minutes.⁷ In the context of VR, threats from online gaming and social media may bleed over from simulated spaces into the real world in new ways. Policymakers and planners may learn to combat metaverse threats from the hazards presented in various online spaces. This thesis draws on parallels between the evolution of online gaming and social media and that of VR and the metaverse.

Metaverse users were surveyed to validate the claim that security threats in the metaverse—extremism, crimes against children, and financial crimes, for example—are not being addressed and that these threats are likely to grow and expand with the metaverse. Additional data from the Center for Countering Digital Hate validate the survey data and the claims of this thesis regarding threats in the metaverse. As the metaverse develops and becomes more sprawling, criminal and terroristic activity will proliferate, and the platform's anonymity and no central point of control will make it particularly difficult for law enforcement to track and identify individuals and their illegal enterprises during investigations.

This thesis emphasizes that law enforcement, the Intelligence Community, and the broader homeland security enterprise should recognize the impending concerns of the metaverse and take steps to be more proactive in addressing potential problems. It recommends enhanced collaboration between industries to secure the metaverse against future threats.

⁵ Angela S. M. Irwin et al., "Money Laundering and Terrorism Financing in Virtual Environments: A Feasibility Study," *Journal of Money Laundering Control* 17, no. 1 (2014): 50–75, <https://doi.org/10.1108/JMLC-06-2013-0019>.

⁶ Choo and Smith, "Criminal Exploitation of Online Systems"; James Cole, "Radicalisation in Virtual Worlds: Second Life through the Eyes of an Avatar," *Journal of Policing, Intelligence and Counter Terrorism* 7, no. 1 (April 2012): 66–79, <https://doi.org/10.1080/18335330.2012.653197>; Irwin et al., "Money Laundering and Terrorism Financing in Virtual Environments"; Caroline Meek-Prieto, "Just Age Playing Around—How Second Life Aids and Abets Child Pornography," *North Carolina Journal of Law & Technology* 9, no. 6 (2008): 88–113, <http://scholarship.law.unc.edu/ncjolt/vol9/iss3/6>.

⁷ Callum Hood, "New Research Shows Metaverse Is Not Safe for Kids," Center for Countering Digital Hate, December 19, 2021, <https://counterhate.com/blog/new-research-shows-metaverse-is-not-safe-for-kids/>.

ACKNOWLEDGMENTS

This thesis is the result of many feverish hours of intense focus and periods of quiet reflection. It would not have been achieved without the help and support of Chris Bellavita, Mollie McGuire, and the entire CHDS–NPS team.

Chris and Mollie, thank you for your unwavering support despite my many anxieties, rantings, and sometimes intense exuberance. Chris, your presence has been paramount, not only through this educational process but also in my personal life; I am forever in your debt. Mollie, thank you for always knowing when it was time to panic and when it was not.

I am so grateful for the opportunity to have participated in this program. To my 2105/2106 classmates, I am a better person for having known you all. “We Got This,” indeed, and there was never a doubt in my mind of that. The resulting friendships and connections, the shared memories, and our cohort’s unique closeness are, in a word, magical.

I would like to thank my family and friends at home for supporting this process over these last 18 months. Without your support system, I could not have succeeded in this venture.

A special thank you and my undying gratitude to Esteban and Rusty for your friendship, encouragement, and steadfast support in this adventure we call life. I hope someday I can return the favor.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The metaverse is a bright new horizon in virtual and augmented reality that carries promise and peril.¹ “Metaverse” refers to a virtual representation of the physical world, usually experienced through a virtual reality (VR) headset. While the metaverse refers broadly to any of the numerous VR worlds that exist on many platforms, the term also applies to Facebook’s 2021 name change to Meta and its specific VR world.² Many possible benefits and problems have begun to develop with the widespread accessibility of “mass-market” VR platforms—as VR has become more widely available at the consumer level, exploitation by bad actors has become more prevalent.³ The metaverse offers a promising outlook for more immersive social experiences online, including anything virtual, from workspaces to travel, to learning, to healthcare.⁴ However, any newly developed piece of technology risks misuse, and in many cases, such abuse is already happening.⁵ The metaverse also poses privacy concerns at government and corporate levels, providing new opportunities for criminal behavior and terrorism, a platform for risky investment strategies including various cryptocurrencies, and many other implications.⁶ In these ways, the future holds imminent threats and benefits.

¹ European Union Agency for Law Enforcement Cooperation, *Policing in the Metaverse: What Law Enforcement Needs to Know* (Luxembourg: Publications Office of the European Union, 2022), <https://data.europa.eu/doi/10.2813/81062>.

² Ling Zhu, *The Metaverse: Concepts and Issues for Congress*, CRS Report No. R47224 (Washington, DC: Congressional Research Service, 2022), <https://crsreports.congress.gov/product/pdf/R/R47224>; Scott Stein, “After a Turbulent 2022, What Happens to Meta’s Metaverse in 2023?,” CNET, December 20, 2022, <https://www.cnet.com/tech/computing/after-a-turbulent-2022-what-happens-to-metas-metaverse-in-2023/>.

³ “Online Abuse in the Metaverse Untangled,” World Wide Web Foundation, February 23, 2022, <https://webfoundation.org/2022/02/online-abuse-in-the-metaverse-untangled/>.

⁴ “Meta for Work: Four Predictions for the Future of Work,” Meta, accessed December 1, 2022, <https://www.meta.com/work/predictions/>; Brian Kalis et al., *Meet Me in the Metaverse: Accenture Digital Health Technology Vision 2022* (Accenture, 2022), <https://www.accenture.com/us-en/insights/health/digital-health-technology-vision>.

⁵ Angus Crawford and Tony Smith, “Metaverse App Allows Kids into Virtual Strip Clubs,” BBC News, February 23, 2022, <https://www.bbc.com/news/technology-60415317>; Tanya Basu, “The Metaverse Has a Groping Problem Already,” *MIT Technology Review*, December 16, 2021, <https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/>.

⁶ Roberto Di Pietro and Stefano Cresci, “Metaverse: Security and Privacy Issues,” in *Proceedings of the Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications* (Piscataway, NJ: IEEE, 2021), 281–88, <https://doi.org/10.1109/TPSISA52974.2021.00032>.

For this thesis, metaverse refers to Meta’s (formerly Facebook’s) VR world. Notably, the metaverse does not necessarily differ in substance from other VR technologies. The marketing of Meta, its intended uses, and widespread applicability differentiate the metaverse from previous implementations of VR.⁷ The military and law enforcement have explored VR from many angles—using it as a training environment and communication platform.⁸ The potential privacy, safety, and security implications affect practitioners from all fields, including law enforcement, the fire service, emergency management, and medical professionals. The metaverse raises many questions about policing, radicalization, healthcare, and various topics at the forefront of homeland security. This virtual world could be a tool for good—to communicate more efficiently, share intelligence, and further protect the homeland—or a tool for nefarious actors—to engage in unsupervised contact with minors, radicalize vulnerable people, or plan attacks undetectable by traditional means.⁹ The metaverse carries risks and benefits, but its successful implementation hinges on policymakers’ preparation.

By examining a survey of metaverse users and reviewing data provided by the Center for Countering Digital Hate, this thesis investigates the nature and prevalence of likely threats in the metaverse. Given its complex virtual environment, understanding the dangers in the metaverse better informs and prepares homeland security professionals and

⁷ Eric Ravenscraft, “What Is the Metaverse, Exactly?,” *Wired*, November 25, 2021, <https://www.wired.com/story/what-is-the-metaverse/>.

⁸ Xinxiong Liu et al., “Virtual Reality and Its Application in Military,” *IOP Conference Series: Earth and Environmental Science* 170, no. 3 (2018): 1–7, <https://doi.org/10.1088/1755-1315/170/3/032155>; David Oliva et al., “Virtual Reality as a Communication Tool for Fire Safety—Experiences from the VirPa Project,” in *Proceedings of the GamiFIN Conference 2019* (CEUR Workshop Proceedings, 2019), 241–52, <http://ceur-ws.org/Vol-2359/paper21.pdf>; Federica Pallavicini et al., “Virtual Reality Applications for Stress Management Training in the Military,” *Aerospace Medicine and Human Performance* 87, no. 12 (2016): 1021–30, <https://doi.org/10.3357/AMHP.4596.2016>; Polona Caserman et al., “A Concept of a Training Environment for Police Using VR Game Technology,” in *Proceedings of the 2018 Joint International Conference on Serious Games*, ed. Stefan Göbel et al., vol. 11243, Lecture Notes in Computer Science (Cham, Switzerland: Springer International Publishing, 2018), 175–81, https://doi.org/10.1007/978-3-030-02762-9_18.

⁹ Will Oremus, “Kids Are Flocking to Facebook’s ‘Metaverse.’ Experts Worry Predators Will Follow,” *Washington Post*, February 7, 2022, <https://www.washingtonpost.com/technology/2022/02/07/facebook-metaverse-horizon-worlds-kids-safety/>; Joel Elson, Austin C. Doctor, and Sam Hunter, “Metaverse, Social Media, Terrorism,” *Homeland Security Newswire*, January 10, 2022, <https://www.homelandsecuritynewswire.com/dr20220110-the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too>.

public safety to protect against threats as the platform gains momentum. Additionally, this thesis explores who, if anyone, is responsible for regulating VR environments.

A. RESEARCH QUESTION

What does the homeland security enterprise need to consider in understanding malicious activity with the increasing usage of the metaverse? This thesis specifically addresses considerations for law enforcement and the Intelligence Community in facing criminal and terroristic activity that might morph from the metaverse into the physical world. Of utmost importance is the exploration of the dangers and threats posed by exploiting the metaverse and how homeland security professionals can begin to approach the problem space.

B. LITERATURE REVIEW

This literature review explores homeland security concerns in pre-metaverse virtual environments. Since limited present-day literature addresses the metaverse specifically, this review treats security threats in other virtual environments, such as Second Life, as a proxy for the crimes and threats of the latest technology. Understanding pre-metaverse virtual environments and the dangers that have plagued them is crucial to anticipating what might emerge from the metaverse. While VR is a “technical system through which a user or multiple users can experience a simulated environment,” virtual environments can extend beyond VR to include all digital settings, for example, computer gaming.¹⁰

Counterintelligence specialists documented homeland security concerns in virtual environments before the metaverse, primarily in the game known as Second Life. Researchers note that radicalization in virtual worlds results from the accessibility of an audience and the volume and availability of terrorist and radical propaganda in a widely

¹⁰ Carina Girvan, “What Is a Virtual World? Definition and Classification,” *Educational Technology Research and Development* 66, no. 5 (October 2018): 1087, <https://doi.org/10.1007/s11423-018-9577-y>.

unregulated environment.¹¹ In this research, Second Life's evolution could be an analog for the metaverse's progression.

Significant research has addressed security concerns in virtual worlds, specifically Second Life's virtual platform. Virtual worlds consist of computer-based simulations that allow users to interact with an environment separate from their physical one. "Multi-user" virtual worlds allow users to interact with the simulated environment and other players.¹² Second Life is one of the leading platforms developed to facilitate this level of social interaction. Researchers have explored radicalization, crimes against children, and even financial crimes all within virtual worlds, but given the time elapsed since the implementation of virtual and augmented reality, they need to probe threats relevant to the metaverse.¹³

Radicalization within Second Life presents a difficult challenge because of its immersive nature. Second Life hosts individual jihadi terrorists and their various groups.¹⁴ Natalie O'Brien's investigation reveals that these groups recruit within Second Life and plan computer-based bombings and terror attacks.¹⁵ Kevin Zuccato, former head of the Australian High Tech Crime Centre, further emphasizes that Second Life facilitates jihadist reconnaissance and surveillance.¹⁶ Additional research asserts the need for intelligence-led capabilities to identify and monitor the terrorist groups operating within virtual spaces. Cole and O'Rourke stress the need to implement counter-radicalization measures in Second

¹¹ James Cole, "Radicalisation in Virtual Worlds: Second Life through the Eyes of an Avatar," *Journal of Policing, Intelligence and Counter Terrorism* 7, no. 1 (April 2012): 66–79, <https://doi.org/10.1080/18335330.2012.653197>.

¹² Ralph Schroeder, "Defining Virtual Worlds and Virtual Environments," *Journal for Virtual Worlds Research* 1, no. 1 (July 2008): 1–3, <https://jvwr-ojs-utexas.tdl.org/jvwr/article/view/294/248>.

¹³ Natalie O'Brien, "Virtual Terrorists," *Australian*, July 31, 2007, Lexis-Nexis; Simon O'Rourke, "Virtual Radicalisation: Challenges for Police," in *Proceedings of the Eighth Australian Information Warfare and Security Conference* (Perth: Edith Cowan University, 2007), <https://doi.org/10.4225/75/57A83C57BEFAB>; Ian Leyden, "How to Tame the New Wild-Wild West: Potential Lassos for Virtual Crime" (South Orange, NJ: Seton Hall University, 2010), https://scholarship.shu.edu/student_scholarship/63.

¹⁴ Cole, "Radicalisation in Virtual Worlds."

¹⁵ O'Brien, "Virtual Terrorists"; O'Rourke, "Virtual Radicalisation."

¹⁶ Lisa Ugelow and Lance Hoffman, "Fighting on a New Battlefield Armed with Old Laws: How to Monitor Terrorism in the Virtual World," *University of Pennsylvania Journal of Constitutional Law* 14, no. 4 (2012): 1035, <https://scholarship.law.upenn.edu/jcl/vol14/iss4/5>.

Life and other virtual worlds but highlight the inherent difficulty.¹⁷ O'Rourke emphasizes the inherent ease with which the internet and virtual worlds facilitate the recruitment, radicalization, and training of terrorist groups with little to no oversight.¹⁸ He further explains that extremist groups isolate individuals from real-world connections and reinforce their new belief system with a unique network of individuals associated with the ideology.¹⁹ Individuals susceptible to radicalization are "made to feel highly valued, and special by their new friends," and "to see themselves as part of a larger, connected community."²⁰ Because of the known threats with Second Life, security professionals must be vigilant in approaching the metaverse.

Additionally, virtual worlds provide criminals and terrorists with a rich environment for real-world financial exploitation. Studies of financial crimes within virtual worlds show that such crimes range from supporting terrorist activity to money laundering and investment schemes. Second Life has its own currency, the Linden dollar, and economy, which enables exploitation. An investment scheme within a game called EVE Online, known as the "Nightfreeze" scam, allegedly cost a user \$1,000.²¹ Irwin and Shay have identified various money laundering and terrorism financing activities in Second Life, including tax evasion, credit card fraud, gold smuggling, and drug trafficking.²² Analyzing the probability of such crimes within virtual environments and the regulatory changes necessary to mitigate them, Irwin and Shay led two real-world terrorism financing and four money laundering conspiracies within two massive multiplayer online games. After anonymizing user identities, the researchers examined and assigned a rating scale to various criteria for the scenarios: how easy it was to exploit the game, how long it took,

¹⁷ Cole, "Radicalisation in Virtual Worlds"; O'Rourke, "Virtual Radicalisation."

¹⁸ O'Rourke, "Virtual Radicalisation."

¹⁹ O'Rourke.

²⁰ O'Rourke, 31.

²¹ "The Great Scam," *Nightfreeze* (blog), accessed June 21, 2022, <http://www.wirm.net/nightfreeze/part1.html>.

²² Angela S. M. Irwin and Jill Slay, "Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft," in *Proceedings of the First International Cyber Resilience Conference* (Perth: Edith Cowan University, 2010), 41–50.

whether detection was likely, and what the plan's cost was.²³ Their analysis showed that in the more robust of the two games, it was possible and even preferential to launder money and finance terrorism using the game rather than other real-world methods. Although all scenarios were technically feasible in the second game, the infrastructure was not robust enough for users to prefer it over real-world schemes. Irwin and Shay's work also highlights the blurred lines between terrorism financing, money laundering, cybercrime, and traditional criminal activity. Most, if not all, crime has a financial link.²⁴ Second Life and EVE Online show that financial crime within virtual worlds is not new, so security professionals can expect the same for the metaverse.

Virtual worlds also provide opportunities for bad actors to exploit children and distribute child pornography. Studies frequently address concerns about crimes against children in the virtual world, running the gamut from privacy violations and misinformation to sexual content, grooming, and groping. Meek-Prieto's and Coleman's research emphasizes how Second Life encourages child pornography.²⁵ Research by Ruiz et al. has found that participants in Second Life have simulated child abuse, represented themselves as children and participated in sexual abuse, and even monetized digital sexual acts.²⁶

Because the metaverse is so new, it remains widely unregulated, and many questions persist about how to handle what happens in this virtual environment. This thesis explicitly addresses concerns and threats to homeland security within the metaverse, such as criminal activity, terrorism, crimes against children, and financial crimes. It also addresses the lack of policy on crimes that occur in virtual environments and bleed over to

²³ Irwin and Slay.

²⁴ Irwin and Slay.

²⁵ Caroline Meek-Prieto, "Just Age Playing Around—How Second Life Aids and Abets Child Pornography," *North Carolina Journal of Law & Technology* 9, no. 6 (2008): 88–113, <http://scholarship.law.unc.edu/ncjolt/vol9/iss3/6>; Sabryne Coleman, "You Only Live Twice: How the First Amendment Impacts Child Pornography in Second Life," *Loyola of Los Angeles Entertainment Law Review* 29, no. 2 (2009): 193–232, <https://digitalcommons.lmu.edu/elr/vol29/iss2/2>.

²⁶ Miguel A. Garcia-Ruiz et al., "Combating Child Exploitation in Second Life," in *Proceedings of the 2009 IEEE Toronto International Conference on Science and Technology for Humanity* (Piscataway, NJ: IEEE, 2009), 761–66, <https://doi.org/10.1109/TIC-STH.2009.5444398>.

the real world and the threat this oversight presents to the homeland. Research has shown that terrorist activity, financial crimes, and crimes against children all have one thing in common—they persist in virtual environments as long as the opportunity exists. Thus, it is vital at the homeland security level to understand the nature of these crimes in the metaverse.

C. RESEARCH DESIGN

This thesis investigates the most salient threats to homeland security posed by the widespread adoption of the metaverse. This research examined existing literature related to homeland security threats in virtual environments—including VR and non-VR platforms such as traditional online gaming—to scrutinize which metaverse-related issues might present themselves and make recommendations on how to combat those issues.

I first examined the evolution of online gaming and its transition to a more social experience. The metamorphosis from online gaming purely for entertainment to a more immersive social networking experience is crucial to understanding the implications of the metaverse. The metaverse, with its intersection of social media, online gaming, and VR, offers an unprecedented opportunity for human connection.²⁷

Then, I conducted a survey of metaverse users, specifically those of social networking apps within the metaverse, about their experiences within the VR world. However, various social networking apps are available on the headset; some are unique to the metaverse while others are cross-platform compatible. Cross-platform compatibility expands the potential for exploiting metaverse applications.

This thesis presents the results of the user experience survey; cross-validates the results with other data, such as game reviews and media reporting; and illustrates the presence of security threats within the metaverse. Then, it discusses strategies for securing the metaverse and future research opportunities.

²⁷ Christine Moy and Adit Gadgil, *Opportunities in the Metaverse: How Businesses Can Explore the Metaverse and Navigate the Hype vs. Reality* (New York: JPMorgan Onyx, 2022), <https://www.jpmorgan.com/content/dam/jpm/treasury-services/documents/opportunities-in-the-metaverse.pdf>.

1. Research Phases

The research design consisted of four phases to map the current threat landscape in the metaverse. Phase 1 reviewed existing literature, studies, and data related to the metaverse and homeland security to better understand the evolution of social media, online gaming, and VR platforms. Phase 1 explored how these technologies have evolved and what the landscape looks like today. This coverage, which provides the reader with the background and progression of the technology, transitions into the discussion of the metaverse. Phase 2 reviewed apps relevant to the metaverse platform to determine which purposes they serve, focusing primarily on apps intended for social networking. For this thesis, social networking apps are open-world and user-driven but do not include games with level progression. This compilation informed which platforms to target in Phase 3.

Phase 3 surveyed users of social platforms within the metaverse to document their experiences and observations in this virtual world. This survey provided baseline data collection to validate whether security threats exist within the metaverse, thus informing future research and policy-planning initiatives. Phase 4 incorporated a discussion on policy planning and implementation to inform critical stakeholders of actions to secure the metaverse, as well as recommendations to combat the ability of bad actors to exploit it.

2. Institutional Review Board

This thesis surveyed users of the metaverse about their experiences in VR. An anonymous survey of VR users using Qualtrics and Amazon's Mechanical Turk was crafted after obtaining Institutional Review Board approval to conduct human subject research. Qualtrics and Amazon's Mechanical Turk deliver surveys across many domains. The questions asked did not induce personally identifiable information, and participants could opt out of the survey at any time. The questions focused on the users' exposure to potentially radicalizing content, sexual content, and financially abusive behavior.

II. ONLINE GAMING AND SOCIAL MEDIA

In recent years, online gaming has undergone explosive growth as entertainment and a tool for social connectivity.²⁸ The COVID-19 pandemic served as a linchpin for some of the most significant transformations of online gaming's use for connectivity and community. Individuals quickly realized that through the shared experience of isolation, they could turn to online gaming to build enduring friendships, relationships, and an entire network of human connections. What once was done in a coffee shop or a networking event could now take place in one's living room, in the comfort of leggings and a hoodie. As Bryan Lufkin attests, gaming has served as a lifeline of sorts for those affected by isolation: "The explosive growth of gaming during the pandemic has shown that many have found a new outlet for much-needed connection in isolation."²⁹

The concept of socializing in an online game is not new but was perhaps underappreciated by a significant portion of the globe before the COVID-19 pandemic. For example, Twitch—a streaming platform that hosts gamers in a live, interactive, video chatroom-style interface—saw record-breaking growth with three billion hours of consumer use in the first quarter of 2020 and five billion hours in the second quarter of 2020.³⁰ Further illustrating the growth of online gaming,

Roblox Corporation says its DAUs [daily active users] now stand at an astonishing 54.7 million, an increase in size of almost exactly a third over January 2021. These players spent 4.2 billion hours on the platform, which is an increase of 26% year over year, and revenue is between \$203 million–\$206 million, up 64%–66% year over year.³¹

²⁸ "3, 2, 1 Go! Video Gaming Is at an All-Time High during COVID-19," Nielsen, June 2020, <https://www.nielsen.com/insights/2020/3-2-1-go-video-gaming-is-at-an-all-time-high-during-covid-19/>.

²⁹ Bryan Lufkin, "How Online Gaming Has Become a Social Lifeline," BBC, December 16, 2020, <https://www.bbc.com/worklife/article/20201215-how-online-gaming-has-become-a-social-lifeline>.

³⁰ Sarah Perez, "Twitch Breaks Records Again in Q2, Topping 5B Total Hours Watched," TechCrunch, July 1, 2020, <https://techcrunch.com/2020/07/01/twitch-breaks-records-again-in-q2-topping-5b-total-hours-watched/>.

³¹ Rich Stanton, "If Roblox's Daily Users Were a Country, It Would Be Bigger than Canada," PC Gamer, February 16, 2022, <https://www.pcgamer.com/if-roblox-daily-users-were-a-country-it-would-be-bigger-than-canada/>.

Such success has not been limited to one platform or one game either. Fortnite, another highly successful platform, has approximately 30 million DAUs, the impact of whom cannot be overstated. The growth of online gaming emphasizes the massive economic and social impact within the United States and globally.

A. GAMING AS A SOCIAL PLATFORM

Increasingly, online and console gaming has become in equal parts a tool for socialization and entertainment. The intersection of social media and online gaming is manifest in social media platforms dedicated to gaming, such as Twitch, Discord, and YouTube. Large gaming communities also use other social media platforms like Reddit and Facebook.³²

Streamers who broadcast content live on the web have quickly become a powerhouse for the videogame industry. Twitch is one of the primary platforms used by streamers to promote content and, more importantly, monetize their time (see Figure 1). One of the most successful streamers on Twitch, Tyler “Ninja” Blevins, makes over \$350,000 a month from his subscribers alone.³³ As of January 2023, Ninja has 18.5 million subscribers on his Twitch channel.³⁴ The most successful streamers often gain sponsorships, have revenue streams of millions of dollars annually, and boast a significant fanbase and merchandise.³⁵

³² r/gaming, “Wiki,” Reddit, accessed January 27, 2023, <https://www.reddit.com/r/gaming/wiki/index/>.

³³ Paul Tassi, “‘Fortnite’ Legend Ninja Talks Twitch Fame and Fortune, and the Game That Got Him There,” *Forbes*, March 13, 2018, <https://www.forbes.com/sites/insertcoin/2018/03/13/fortnite-legend-ninja-talks-twitch-fame-and-fortune-and-the-game-that-got-him-there/>.

³⁴ Ninja, “Jujutsu Kaisen Collab Is in Fortnite All Day Games around 10am Central w/Timthetatman and Cloakzy,” Twitch, accessed January 24, 2023, <https://www.twitch.tv/ninja>.

³⁵ Cynthia Bowman, “How Much Do Twitch Streamers Make? 2023 Top Earners,” GO Banking Rates, April 27, 2023, <https://www.gobankingrates.com/money/entrepreneur/how-much-do-twitch-streamers-make/>.



Figure 1. Total Hours Streamed on Twitch.³⁶

Online gaming allows young people and teenagers to socialize with their peers and make new friends and connections.³⁷ In their research about the impact of video games on children's relationships, Amanda Lenhart et al. have found,

Video games and gameplay are pervasive in the lives of most American teens—and for boys in particular, video games serve as a major venue for creating and maintaining friendships. . . . Many teens play games with pals as part of in-person friendships. But teens also play with people they know only online. Among boys and girls who play games with others over a network, 90% of networked-gaming boys and 85% of girls are playing these games with friends they know in person (for a total of 89% of all teens).³⁸

³⁶ Source: Perez, "Twitch Breaks Records Again in Q2."

³⁷ Amanda Lenhart et al., "Chapter 3: Video Games Are Key Elements in Friendships for Many Boys," in *Teens, Technology & Friendships: Video Games, Social Media and Mobile Phones Play an Integral Role in How Teens Meet and Interact with Friends* (Washington, DC: Pew Research Center, 2015), <https://www.pewresearch.org/internet/2015/08/06/chapter-3-video-games-are-key-elements-in-friendships-for-many-boys/>.

³⁸ Lenhart et al., 41, 44.

Using online games to facilitate friendship emphasizes the importance of technology in modern-day relationships and socialization. This phenomenon will be particularly relevant as the technology evolves and becomes a more immersive experience for the end user.

B. CRIMINAL ACTIVITY IN SOCIAL MEDIA AND ONLINE GAMING

A slew of factors complicates the intersection of crime and the internet. For as long as online gaming has existed, it has also facilitated illegal activity.³⁹ Most communities exist for social good and cohesion, yet criminals exploit unique opportunities in online gaming. In many cases, the crimes perpetuated online are financial or have a financial connection to the physical or natural world.⁴⁰ Other examples include harassment, stalking, child exploitation, bullying, and revenge porn.⁴¹ Investigating criminal activity in emerging technologies has long plagued law enforcement, and online gaming is no different.⁴² Myriad issues at the organizational and strategic levels have prevented law enforcement and intelligence officials from keeping pace—inconsistent policies across the 18,000 law enforcement organizations, concerns about civil rights and civil liberties, and government surveillance of open-source information are just a few.⁴³ Law enforcement has notoriously fallen behind the evolution of technology, and efforts to be more proactive are stilted at best.

Online gaming is no different from other online communities in providing even the most disadvantaged with a voice—considering the internet is the great equalizer. The

³⁹ Kim-Kwang Raymond Choo and Russell G. Smith, “Criminal Exploitation of Online Systems by Organised Crime Groups,” *Asian Journal of Criminology* 3, no. 1 (June 2008), <https://doi.org/10.1007/s11417-007-9035-y>; Matthew S. Ruskin, “Playing in the Dark How Online Games Provide Shelter for Criminal Organizations in the Surveillance Age,” *Arizona Journal of International & Comparative Law* 31, no. 3 (2014), <http://arizonajournal.org/wp-content/uploads/2015/09/10-Ruskin.pdf>.

⁴⁰ Angela S. M. Irwin et al., “Money Laundering and Terrorism Financing in Virtual Environments: A Feasibility Study,” *Journal of Money Laundering Control* 17, no. 1 (2014): 50–75, <https://doi.org/10.1108/JMLC-06-2013-0019>.

⁴¹ Choo and Smith, “Criminal Exploitation of Online Systems”; Cole, “Radicalisation in Virtual Worlds”; Irwin et al., “Money Laundering and Terrorism Financing in Virtual Environments”; Meek-Prieto, “Just Age Playing Around.”

⁴² European Union Agency for Law Enforcement Cooperation, *Policing in the Metaverse*.

⁴³ “3 Roadblocks for Using OSINT in Law Enforcement,” *Authentic8* (blog), April 27, 2022, <https://authentic8.com/blog/3-roadblocks-using-osint-law-enforcement>; European Union Agency for Law Enforcement Cooperation, *Policing in the Metaverse*.

implication is that a community exists for everyone, available at one's fingertips without needing a physical presence. Not only does increased networking give criminals, extremists, and terrorists a voice online; it also helps them recruit others to their ideology, undetected by traditional law enforcement techniques. For the most part, the internet allows users to express their beliefs, no matter how morally unconscionable. Thus, extremists and individuals on the fringes of society find each other and create robust communities.⁴⁴ Such cohesion in social media and gaming communities provides a unique opportunity for extremists to share their belief systems and develop relationships with vulnerable individuals, including children, to radicalize and recruit them.⁴⁵ The feeling of camaraderie, especially when an individual is physically isolated, is powerful and sets the stage for influence. Although extremist content is not illegal—jurisdictional differences aside—it is still a cause for concern among law enforcement and intelligence professionals.

The following terms, often used when discussing online gaming, provide context for the subsequent discussion:

- *Sandbox* or *creation games* are a category of online games that gives players various creative tools and allows them to place all their assets in one place (a sandbox).⁴⁶
- *Non-player controlled* (NPC) entities are typically humanoid or animal characters whose behaviors are pre-programmed or customizable. NPCs require no players to perform actions.⁴⁷
- A *private server capability* permits a single person or group to join a private game together without moderation or oversight, either hosted

⁴⁴ Willem De Koster and Dick Houtman, "'Stormfront Is Like a Second Home to Me': On Virtual Community Formation by Right-Wing Extremists," *Information, Communication & Society* 11, no. 8 (2008): 1155–76, <https://doi.org/10.1080/13691180802266665>.

⁴⁵ O'Rourke, "Virtual Radicalisation."

⁴⁶ *Merriam-Webster*, s.v. "sandbox," accessed January 23, 2023, <https://www.merriam-webster.com/dictionary/sandbox>.

⁴⁷ Chrissy Montelli, "What Does 'NPC' Mean? Understanding Non-player Characters, an Important Aspect of Any Video Game," *Insider*, May 28, 2021, <https://www.businessinsider.com/guides/tech/npc-meaning>.

directly on one's home network or rented via a third-party provider. Thus, it may be possible to track the home server's internet protocol (IP) to a physical address using open-source resources.⁴⁸

- *Raging* involves behaviors usually caused by another player or a difficult game mechanic that halts the player's process, causing frustration.⁴⁹ This reaction may include quitting the game or even having a physical response, such as throwing a controller or breaking equipment.⁵⁰
- *Swatting* is a dangerous prank in which a frustrated player procures a victim's physical address from an IP address and contacts the local police department to report an active hostage situation that warrants a police response to breach the victim's house.⁵¹

1. Roblox

One viral game, Roblox, initially designed for children, has rapidly become a breeding ground for extremist content.⁵² Roblox is both a sandbox game and a platform game. The emphasis on community distinguishes Roblox and similar games from more traditional gaming experiences. These games have chat and friendship features and the ability to participate in gameplay without being constrained to specific goals, achievements, and level advancement. The game allows users a significant degree of freedom to play how and when they choose without mandating an order of operations. The sandbox style of online gaming has become more popular as consumers have used it for

⁴⁸ Stephen Kish, "Massive Multiplayer Games a Platform for Terrorism?," Patrick Henry College, May 17, 2017, <https://www.phc.edu/intelligencer/massive-multiplayer-games-a-platform-for-terrorism>.

⁴⁹ Juho Kahila et al., "Gamer Rage—Children's Perspective on Issues Impacting Losing One's Temper While Playing Digital Games," *International Journal of Child-Computer Interaction* 33 (September 2022): 100513, <https://doi.org/10.1016/j.ijcci.2022.100513>.

⁵⁰ Kahila et al.

⁵¹ "What Is Swatting? How to Prevent Swatting," Cloudflare, accessed January 26, 2023, <https://www.cloudflare.com/learning/security/glossary/what-is-swatting/>.

⁵² Cyrus Farivar, "Extremists Creep into Roblox, an Online Game Popular with Children," NBC News, August 21, 2019, <https://www.nbcnews.com/tech/tech-news/extremists-creep-roblox-online-game-popular-children-n1045056>.

social experiences rather than for achievement, level progression, or a way to beat the game.⁵³ This open-ended environment allows for more user-driven content and decision-making, creating the risk of bad actors exploiting the environment.

Minors are particularly susceptible to victimization online by extremist recruiting or child sexual exploitation. Unsupervised children have free-range access to online communities, particularly those associated with online gaming. Industries frequently coerce children into online spaces, and when parents ignore content ratings and warnings, little can be done to prevent such exposure.⁵⁴ Roblox has three age content ratings: all ages, 9 and older, and 13 and older.⁵⁵ These age ratings serve as guidelines for parents of young children, but they are not foolproof: children are still exposed to violent and unsafe material on the platform.

Since the advent of the world wide web, criminals have used online gaming, social media, and, more broadly, the internet to foster environments conducive to their nefarious activities. Online gaming and social media facilitate suspicious behavior and conceal illegal activity, including financial crimes, extremism, and explicit content.⁵⁶ Online gaming provides a platform for individuals to exhibit emotionally dysregulated behavior. Users may send hate speech to players they have interacted with on these platforms, provided their privacy settings permit such contact.

Online gaming platforms also allow individuals to covertly perpetrate suspicious activities that have been observable traditionally in the real world. The Nationwide

⁵³ Kurt Squire, "Open-Ended Video Games: A Model for Developing Learning for the Interactive Age," in *The Ecology of Games: Connecting Youth, Games, and Learning*, ed. Katie Salen (Cambridge, MA: MIT Press, 2008), <https://doi.org/10.1162/dmal.9780262693646.167>.

⁵⁴ "Internet Use in Children," American Academy of Child and Adolescent Psychiatry, October 2015, https://www.aacap.org/AACAP/Families_and_Youth/Facts_for_Families/FFF-Guide/Children-Online-059.aspx; Melinda Wenner Moyer, "Kids as Young as 8 Are Using Social Media More than Ever, Study Finds," *New York Times*, March 24, 2022, <https://www.nytimes.com/2022/03/24/well/family/child-social-media-use.html>.

⁵⁵ "Experience Guidelines and Age Recommendations," Roblox Support, accessed January 19, 2023, <https://en.help.roblox.com/hc/en-us/articles/8862768451604-Age-Recommendations>.

⁵⁶ Anti-Defamation League, *Hate Is No Game: Harassment and Positive Social Experiences in Online Games 2021* (New York: Anti-Defamation League, 2021), <https://www.adl.org/resources/report/hate-no-game-harassment-and-positive-social-experiences-online-games-2021>.

Suspicious Activity Reporting Initiative publishes a list of defined criminal activities as well as potential indicators of such schemes (see Figure 2).⁵⁷ While public safety professionals in the United States are trained to observe these activities and indicators in public spaces, identifying these behaviors in online spaces, especially role-playing games, can be challenging for even the most seasoned investigator.

⁵⁷ “Suspicious Activity Reporting Indicators and Behaviors,” Nationwide SAR Initiative, February 2016, https://www.dhs.gov/sites/default/files/publications/16_0208_NSI_SAR-Indicators-Behaviors-Tools-Analysts-Investigators.pdf.



Suspicious Activity Reporting Indicators and Behaviors

Tools for
Analysts and
Investigators

Behaviors

Descriptions

Defined Criminal Activity and Potential Terrorism Nexus Activity

Breach/Attempted Intrusion	Unauthorized personnel attempting to enter or actually entering a restricted area, secured protected site, or nonpublic area. Impersonation of authorized personnel (e.g., police/security officers, janitor, or other personnel).
Misrepresentation	Presenting false information or misusing insignia, documents, and/or identification to misrepresent one's affiliation as a means of concealing possible illegal activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure or secured protected site (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents (classified or unclassified)), which are proprietary to the facility/infrastructure or secured protected site.
Sabotage/Tampering/Vandalism	Damaging, manipulating, defacing, or destroying part of a facility/infrastructure or secured protected site.
Cyberattack	Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to commit a crime that will result in death or bodily injury to another person or persons or to damage or compromise a facility/infrastructure or secured protected site.
Aviation Activity	Learning to operate, or operating an aircraft, or interfering with the operation of an aircraft in a manner that poses a threat of harm to people or property and that would arouse suspicion of terrorism or other criminality in a reasonable person. Such activity may or may not be a violation of Federal Aviation Regulations.

Potential Criminal or Non-Criminal Activities Requiring Additional Information During Vetting

Note: When the behavior describes activities that are not inherently criminal and may be constitutionally protected, the vetting agency should carefully assess the information and gather as much additional information as necessary to document facts and circumstances that clearly support documenting the information as an ISE-SAR.

Eliciting Information	Questioning individuals or otherwise soliciting information at a level beyond mere curiosity about a public or private event or particular facets of a facility's or building's purpose, operations, security procedures, etc., in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Recruiting/Financing	Providing direct financial support to operations teams and contacts or building operations teams and contacts; compiling personnel data, banking data, or travel data in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Photography	Taking pictures or video of persons, facilities, buildings, or infrastructure in an unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include taking pictures or video of infrequently used access points, the superstructure of a bridge, personnel performing security functions (e.g., patrols, badge/vehicle checking), security-related equipment (e.g., perimeter fencing, security cameras), etc.
Observation/Surveillance	Demonstrating unusual or prolonged interest in facilities, buildings, or infrastructure beyond mere casual (e.g., tourists) or professional (e.g., engineers) interest and in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include observation through binoculars, taking notes, attempting to mark off or measure distances, etc.
Materials Acquisition/Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, radio control toy servos or controllers; fuel, chemicals, or toxic materials; and timers or other triggering devices, in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Acquisition of Expertise	Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Weapons Collection/Discovery	Collection or discovery of unusual amounts or types of weapons, including explosives, chemicals, and other destructive materials, or evidence, detonations or other residue, wounds, or chemical burns, that would arouse suspicion of terrorism or other criminality in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (e.g., the public health sector), with regard to their personnel, facilities, systems, or functions in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.

<http://nsi.ncirc.gov>

rev. 02/16

Figure 2. Suspicious Activity Reporting Indicators and Behaviors.⁵⁸

⁵⁸ Source: Nationwide SAR Initiative.

Online role-playing (RP) games usually involve a collection of people who share a specific interest on a single server where everyone plays a part in a written narrative. RP games can also encompass the portrayal of a particular group or individual. A game server functions as the computer framework, meaning the space where the game is hosted and from which it operates. An example of RP includes military games on multiple platforms that allow players to create soldiers, join squads or units, and engage in battles with other teams. While RP gaming can be a harmless expression, the open practice of more violent behaviors also exists. Some games allow players to partake in mass-shooting events, maintain deep cover within a terrorist organization, or participate in school shootings and other behaviors that emulate a mass attack's planning and preparation phases.⁵⁹ The ability for players to emulate these attacks and other violent content can be used in the planning and preparation of real-world attacks.

Organized hate groups operate online to spread their ideology more efficiently than in the real world and reduce the potential of interception by law enforcement. They also operate on these platforms, using them as recruitment opportunities or ways to meet and spread their ideology undetected.⁶⁰ Among such groups, racially motivated violent extremists (RMVEs) most commonly use online gaming platforms to operate in these ways; however, with the introduction of RP in online games, these borders have expanded.⁶¹ Now, any individuals with malicious intent can use these spaces as force multipliers to spread their beliefs and intentions, gain support, and even recruit others to join their cause.

Another complicating factor for law enforcement is the widespread use of VR platforms. Mass-market VR headsets are becoming commercially available, and significant research gaps exist about the implications for law enforcement and homeland security

⁵⁹ James Troughton, "Roblox Is Cracking Down on Players Recreating School Shootings in-Game," *Gamer*, August 19, 2021, <https://www.thegamer.com/roblox-school-shootings/>.

⁶⁰ "Examining the Intersection between Gaming and Violent Extremism: Executive Summary," United Nations Counter-Terrorism Centre, accessed January 26, 2023, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/221005_execute_summary_on_gaming_ve.pdf.

⁶¹ Kish, "A Platform for Terrorism?"

professionals. Various reports of crime in the metaverse are becoming more frequent and more severe, drawing attention to the potential consequences of such technology. Discussions of crime beginning in the metaverse and bleeding over to the real world are also increasing.⁶² Several games have unintentionally allowed this practice to prosper by allowing players to host private servers paired with a creation engine or sandbox to create any scenario they wish. Law enforcement and public safety professionals should understand sandbox platforms when exploring ways that bad actors can use gaming and VR.

2. Second Life

One of the first and largest open-ended virtual worlds to become widely successful is Second Life.⁶³ Originating in 2003, Second Life quickly gained traction in the real world by establishing a virtual economy, social spaces, and complex virtual environments.⁶⁴ Users created an avatar and assumed an identity to represent themselves among millions of other users in an interactive environment.⁶⁵ Second Life was undoubtedly more than an online game, but articulating the world's comprehensiveness is challenging. Linden Labs, the creator of Second Life, argued that Second Life was anything but a game. "There is no manufactured conflict, no set objective," said spokesperson Catherine Smith in 2007. "It's an entirely open-ended experience."⁶⁶ Without an end objective for users to play through and complete, the environment became a digital representation of the real world, used for socialization and to facilitate human interaction.

In many ways, Second Life mirrored the real world: a robust economy, social interaction, and more. It allowed individuals to create virtual representations, or avatars, of

⁶² Michael Kan, "Police in the Metaverse? Interpol Urges Law Enforcement to Embrace VR Tech," *PC Magazine*, October 21, 2022, <https://www.pcmag.com/news/police-in-the-metaverse-interpol-urges-law-enforcement-to-embrace-vr-tech>.

⁶³ "Home Page," Second Life, accessed January 26, 2023, <https://secondlife.com/>.

⁶⁴ Kristin Kalning, "If Second Life Isn't a Game, What Is It?," NBC News, March 11, 2007, <https://www.nbcnews.com/id/wbna17538999>.

⁶⁵ Toin Villar, "What Is Second Life? A Brief History of the Metaverse," Make Use Of, April 11, 2022, <https://www.makeuseof.com/what-is-second-life-history-metaverse/>.

⁶⁶ Kalning, "If Second Life Isn't a Game, What Is It?"

themselves and interact with other people through their avatars, physical places, and objects.⁶⁷ The virtual economy within Second Life has rested on the Linden dollar, exchangeable for the U.S. dollar based on a floating rate.⁶⁸ Using the Linden dollar, users could do many things virtually that they could do in the real world: purchase land, build homes, purchase clothing or any other items, or communicate with friends.⁶⁹ While relatively innocuous, the mirror world also set the stage for more nefarious activity in Second Life.

Second Life demonstrated latent criminal opportunities that might foreshadow crimes in the metaverse. At its 2007 peak, Second Life experienced average monthly users of nearly 1.1 million, which declined after that. During the COVID-19 pandemic, monthly users surged to 900,000.⁷⁰ Second Life was one of the precursors to the modern-day metaverse; in that way, it also saw its share of criminal and extremist activity. Crimes in Second Life have run the gamut of child exploitation, intellectual property theft, financial scams, and even terrorism.⁷¹ The existence of these crimes in Second Life serves as an important prediction of future crimes in other virtual environments.

James Cole researched the simplicity of radicalization within online environments such as Second Life.⁷² After creating a Second Life avatar, Cole began exploring various worlds focused on black bloc tactics, protest movements, and eventually extremist content.

⁶⁷ Simon Gottschalk, "The Presentation of Avatars in Second Life: Self and Interaction in Social Virtual Spaces," *Symbolic Interaction* 33, no. 4 (2010): 501–25, <https://doi.org/10.1525/si.2010.33.4.501>.

⁶⁸ "What Is the Linden Dollar?," Investopedia, accessed January 26, 2023, <https://www.investopedia.com/terms/l/linden-dollar.asp>.

⁶⁹ "Second Life: Facts for the Visitor," *Wired*, October 1, 2006, <https://www.wired.com/2006/10/slfacts/>.

⁷⁰ "Second Life Usage Now Higher than Its 2007 Hype Level Period?," *New World Notes* (blog), June 22, 2020, <https://nwn.blogs.com/nwn/2020/06/second-life-sl-linden-lab-mau-concurrency.html>.

⁷¹ Chris Gourlay and Abul Taher, "Virtual Jihad Hits Second Life website," *Times* (United Kingdom), August 5, 2007, <https://www.thetimes.co.uk/article/virtual-jihad-hits-second-life-website-l2cf6vm92pb>; Meek-Prieto, "Just Age Playing Around"; Robert Stokes, "Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar," *Information & Communications Technology Law* 21, no. 3 (2012): 221–36, <https://doi.org/10.1080/13600834.2012.744225>; Cole, "Radicalisation in Virtual Worlds"; Sinclair Jeter and Darris Taylor, "Terrorist Presence in Virtual Worlds : Using Second Life as a Case Study," *International Journal of Interdisciplinary Social Sciences: Annual Review* 6, no. 10 (2012): 1–6, <https://cgscholar.com/bookstore/works/terrorist-presence-in-virtual-worlds>.

⁷² Cole, "Radicalisation in Virtual Worlds," 66–79.

Through his avatar, Farid, Cole used keyword searches such as “Muslim,” “mosque,” “Islam,” and others, to choose a world and then travel to its library, which linked to websites and Facebook pages outside Second Life. Also visible in the library were books that promoted “extremist views of Islam” and more external links.⁷³ Cole found

a site containing statements in favour of the mujahedeen and providing direct downloads of texts such as *How to Save the World* written by Osama bin Laden and other texts attributed to bin Laden and other al-Qaeda members. The lone avatar’s profile gives its name as ALFaruokiOmari and indicates it is a member of the Taliban group “(Al-Qaeda-Taliban) the right path.”⁷⁴

Second Life provided a foundation for participants to radicalize using a few keyword searches and navigate to external sites. Individuals already vulnerable to radicalization could be even more susceptible within the game’s social aspect. Cole has pointed out that how far an individual goes in these acts depends entirely on one’s unique circumstances.

In the same way Second Life was susceptible to criminal and extremist activity; it was also prone to complicate investigations by law enforcement. One complication involved the jurisdictional challenges of the global platform, with perpetrators and victims separated by thousands of miles. As far back as 2007, the BBC investigated allegations of virtual child pornography (digital avatars depicting children) in Second Life, something not prohibited in the United States but punishable in Germany by three years in prison.⁷⁵ A 2002 Supreme Court ruling highlighted another complicating factor in such criminal investigations into Second Life:

In 2002, *Ashcroft v. Free Speech Coalition* held that the possession, creation, or distribution of “virtual child pornography,” pornography created entirely through computer graphics, was not a punishable offense because regulation impermissibly infringed on the First Amendment right to free speech and did not harm real children.⁷⁶

⁷³ Cole.

⁷⁴ Cole.

⁷⁵ “Second Life ‘Child Abuse’ Claim,” BBC News, May 9, 2007, <http://news.bbc.co.uk/2/hi/technology/6638331.stm>.

⁷⁶ Meek-Prieto, “Just Age Playing Around.”

The *Ashcroft* ruling and subsequent complications are harbingers of similar legal difficulties for crime and free speech within virtual spaces.

C. CONCLUSION

Law enforcement has faced significant challenges in identifying, investigating, and prosecuting bad actors within virtual spaces. There is no legal framework in place for addressing such criminal activities as of this writing.⁷⁷ Governments find themselves in a tricky situation with jurisdictional boundaries in the virtual realm. Because physical borders do not bind virtual worlds, determining which countries' or jurisdictions' laws apply to activities within the metaverse will pose grave challenges for law enforcement.

⁷⁷ Shawn Ray, "The Metaverse Is Coming—Who Will Police It?," Police1, January 30, 2023, <https://www.police1.com/investigations/articles/the-metaverse-is-coming-who-will-police-it-ttPcF7hT9wrhfvha/>.

III. BACKGROUND OF VIRTUAL REALITY

This chapter establishes the magnitude and growth of the metaverse, laying the foundation for a subsequent discussion of the latent threats this platform holds. Accordingly, this chapter covers the origins of VR, critical terms and concepts, pre-Oculus VR technologies, and the origins of the metaverse.

A. VIRTUAL REALITY ORIGINS AND CRITICAL TERMS

Pioneered as the Sword of Damocles, the first mentions of VR were by Ivan Sutherland in 1968.⁷⁸ The system was so heavy that it had to be anchored to the ceiling of his research lab, but a physical representation of VR was born (see Figure 3). Long before Sutherland's physical headset, science fiction stories spawned the idea of a futuristic device that allowed an individual to exist in a reality different from one's own.

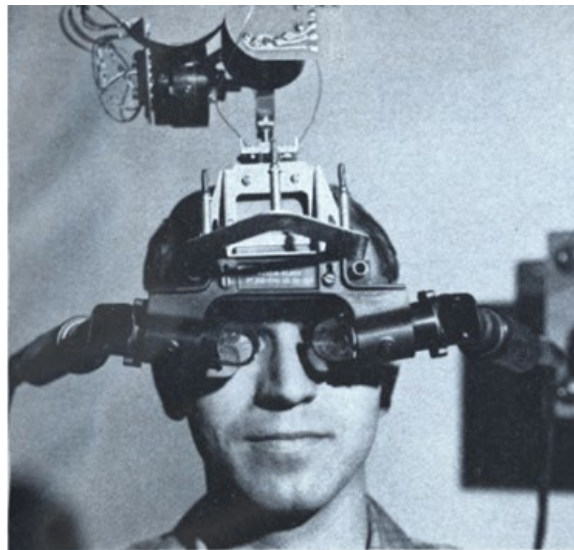


Figure 3. Sword of Damocles.⁷⁹

⁷⁸ Georgi Yordanov Kostov, "Fostering Player Collaboration within a Multimodal Co-located Game" (master's thesis, University of Applied Sciences Upper Austria, Hagenberg, 2015), 5, fig. 2.2, https://www.researchgate.net/figure/The-Sword-of-Damocles-by-Ivan-Sutherland_fig2_291516650.

⁷⁹ Source: Kostov, 5, fig. 2.2.

Several decades of work led to the VR technologies that have been made widely available in the 21st century. In the 1970s, inventors at GE, MIT, and McDonnell-Douglas made some of the first developments. In the late 1980s, NASA entered the field of VR. In the 1990s, VR arcade machines became mainstream, and Sega announced its release of VR glasses. By the same token, in 2012, a Kickstarter campaign was launched for the Oculus headset, one of the most well-known VR headsets today. In 2014, Facebook, since rebranded as Meta, purchased the Oculus headset for \$2 billion.⁸⁰ At this time, several other companies, such as Sony and HTC, began breaking into the VR market, marking the beginning of the race for best in VR. From 2017 to 2019, VR became the new fad product. Oculus, now Meta, headsets were in high demand.⁸¹ Various independent app developers created VR experiences, ranging from roller coasters to horror games to meditation, denoting this fad's mass popularization.⁸²

Defining VR experiences includes an individual psychological component beyond the actual technology represented. In *Communication in the Age of Virtual Reality*, Jonathan Steuer aptly describes this effect:

The key to defining virtual reality in terms of human experience rather than technological hardware is the concept of presence. Presence can be thought of as the experience of one's physical environment; it refers not to one's surroundings as they exist in the physical world, but to the perception of those surroundings.⁸³

Steuer uses "presence" to articulate plainly the human experience in virtual worlds and to explain its gravitas. In describing presence within virtual environments, he focuses on the concept of immersion, which consists of the depth and breadth of information in the virtual

⁸⁰ "Oculus Acquired by Meta," Crunchbase, accessed March 6, 2023, <https://www.crunchbase.com/acquisition/facebook-acquires-oculus-vr--30357598>.

⁸¹ Dave Johnson, "The Oculus Quest Is Sold Out Pretty Much Everywhere Right Now," CNET, September 9, 2020, <https://www.cnet.com/deals/where-you-can-buy-hard-to-find-oculus-quest-right-now/>.

⁸² "History of Virtual Reality," Virtual Reality Society, accessed September 21, 2022, <https://www.vrs.org.uk/virtual-reality/history.html>.

⁸³ Jonathan Steuer, "Defining Virtual Reality: Dimensions Determining Telepresence," in *Communication in the Age of Virtual Reality*, ed. Frank Biocca and Mark R. Levy (Hillsdale, NJ: Lawrence Erlbaum Associates, 1995), 35.

space.⁸⁴ The depth of information refers to the technical specifications of the VR system while the breadth of information refers to “sensory dimensions presented simultaneously.”⁸⁵ Put simply, immersion can be thought of as the degree to which one’s brain perceives the virtual environment as real. For example, the level of immersion would determine whether the user views a room through a window or experiences the room from inside it. Someone fully immersed in VR might report all one’s senses being engaged in the virtual world.

Furthermore, other factors affect the level of immersion. According to Slater and Wilbur, “Sense of presence, or the perceptual experience of being in a VE [virtual environment], is a function of level of immersion mediated by the context of a task and the perceptual thresholds of the participant.”⁸⁶ Brown and Cairns assert that “full immersion is presence,” highlighting the influence that manipulation of the immersion level may have on a user’s experience.⁸⁷ These two concepts are distinct in that immersion refers to technical manipulations while presence refers to a user’s experience. However, since the level of immersion facilitates the sense of presence, which in turn moderates learning effects, it is impossible to completely dissociate these constructs.⁸⁸

Enhancements to the virtual world allow users to experience physical sensations as though they are truly in the environment. Many accessories paired with a VR headset, including vests, gloves, pants, and platforms that map the virtual world, can bolster

⁸⁴ “Virtual Reality Immersion,” Virtual Reality Society, accessed January 26, 2023, <https://www.vrs.org.uk/virtual-reality/immersion.html>.

⁸⁵ Virtual Reality Society.

⁸⁶ Mel Slater and Sylvia Wilbur, “A Framework for Immersive Virtual Environments (FIVE): Speculations on the Role of Presence in Virtual Environments,” *Presence: Teleoperators and Virtual Environments* 6, no. 6 (1997): 603–16, <https://doi.org/10.1162/pres.1997.6.6.603>; Bob G. Witmer and Michael J. Singer, “Measuring Presence in Virtual Environments: A Presence Questionnaire,” *Presence: Teleoperators and Virtual Environments* 7, no. 3 (1998): 225–40, <https://doi.org/10.1162/105474698565686>.

⁸⁷ Emily Brown and Paul Cairns, “A Grounded Investigation of Game Immersion,” in *CHI '04 Extended Abstracts on Human Factors in Computing Systems* (New York: Association for Computing Machinery, 2004), 1297–1300, <https://doi.org/10.1145/985921.986048>.

⁸⁸ Haylie L. Miller and Nicoleta L. Bugnariu, “Level of Immersion in Virtual Environments Impacts the Ability to Assess and Teach Social Skills in Autism Spectrum Disorder,” *Cyberpsychology, Behavior and Social Networking* 19, no. 4 (2016): 246–56, <https://doi.org/10.1089/cyber.2014.0682>.

immersion within virtual environments.⁸⁹ The wearable accessories often contain sensors and vibrating parts that simulate touching, pushing, or shoving, also known as haptics (see Figures 4–5).⁹⁰ The platforms allow the user to move around a virtual world more extensively than the physical space that one inhabits (see Figure 6).⁹¹ There are many uses for these types of experiences; one includes first-person shooter games, where the user carries a VR controller that looks like a rifle. Still, within the headset, the user may be running across a desert warzone, covering a distance far greater than the physical area the user occupies. Thus, users can act as heroes in their own stories without threat of physical harm. Examples of immersive haptic devices compatible with Meta Quest headsets appear in Table 1.



Figure 4. bHaptics VR Vest.⁹²

⁸⁹ Andre Oentoro, “5 VR Accessories You Need for the Next-Level Immersion,” AR Post, July 27, 2022, <https://arpost.co/2022/07/27/5-vr-accessories-next-level-immersion/>; “Home Page,” Omnifinity, accessed January 26, 2023, <https://www.omnifinity.se/>.

⁹⁰ “Home Page,” bHaptics, accessed January 26, 2023, <https://www.bhaptics.com/>.

⁹¹ Omnifinity, “Home Page.”

⁹² Source: bHaptics, “Home Page.”



Figure 5. bHaptics VR Vest Feedback Points.⁹³



Figure 6. Omnifinity's Omnidirectional VR Platform.⁹⁴

⁹³ Source: bHaptics.

⁹⁴ Source: Omnifinity, "Omnideck 6 at I/ITSEC 2014," video, 1:19, YouTube, December 1, 2014, <https://www.youtube.com/watch?v=wPffziOrE6Y>.

Table 1. Immersive Haptic Devices for Use with Meta Quest Headsets.⁹⁵

Haptic suit	At the heart of immersive technology are wearable suits such as the TESLASUIT, which can allow the user to experience real-world sensations of touch, from the feeling of raindrops to the impact of blunt force. ⁹⁶ Currently the TESLASUIT sells for \$12,999. ⁹⁷
Haptic gloves	Through the use of an exoskeleton, TESLASUIT XR gloves create resistance, providing the perception of the shape, size and density of virtual objects. Its current cost is \$14,999. ⁹⁸
Eyewear/goggles	Immersive goggles provide a 360-degree immersive view in the virtual world. Through technological advancements, goggles such as the Meta Quest Pro are lightweight and display the wearer's facial expressions on their avatar. The Meta Quest Pro is available for \$1,499. ⁹⁹
Miscellaneous devices	The KAT Walk C 2 Personal VR Treadmill provides 360 degrees of natural movement. It costs \$1,099. ¹⁰⁰
Olfactometer devices	These can emit various scents to the user, which will be utilized in future haptic devices to create taste in the virtual world. Several companies have working prototypes.

B. PRE-OCULUS VR GAMING

Several platforms existed before the Meta Quest (formerly Oculus) headset and Meta's metaverse. These platforms helped build the foundation for future VR (see Table 2). In 2016, Sony released a VR headset compatible with the PlayStation 4 and PlayStation

⁹⁵ Source: Ray, "The Metaverse Is Coming." Table 1 retains the sources cited in the original article.

⁹⁶ Bobby Carlton, "Feel Rain Fall in VR with Full-Body Teslasuit," VR Scout, July 12, 2021, <https://vrscout.com/news/feel-rain-fall-in-vr-with-full-body-teslasuit/>.

⁹⁷ "Home Page," Teslasuit, accessed April 18, 2023, <https://teslasuit.io/>.

⁹⁸ Teslasuit.

⁹⁹ "This Is Meta Quest Pro," Meta, accessed April 18, 2023, <https://www.meta.com/quest/quest-pro/>.

¹⁰⁰ "KAT Walk C2 Core," KAT VR, accessed April 18, 2023, <https://www.kat-vr.com/products/kat-walk-c2>.

5. Valve has developed a PC-tethered VR system with particularly immersive controllers, allowing users to use their hands exactly as they do in the real world. Vive's headset, the Vive Pro, has advanced eye tracking, room tracking, and impressive technological specifications.

Table 2. VR Headset Comparison.¹⁰¹

THE WILD IMMERSIVE COLLABORATION FOR TEAMS 2022 Business VR Headset Comparison Chart (Q1)						
	Meta Quest 2	Pico Neo 3	HP Reverb G2	Valve Index	Vive Pro 2	Vive Pro
						
Official Support in The Wild						
Resolution / Eye	1832 x 1920	1832 x 1920	2160x2160	1440x1600	2448 x 2448	1440x1600
Refresh Rate (HZ)	90/120	90	90	144	120	90
Field of View	100°	98°	114°	130°	120°	110°
Weight	503g	620g	544g	570g	850g	563g
Tracking	Inside-out	Inside-out	Inside-out	Base Stations (more equipment = more precise hand tracking)	Base Stations (more equipment = more precise hand tracking)	Base Stations (more equipment = more precise hand tracking)
Type	Standalone (no wires, less powerful processor) + option to wirelessly stream or tether to a PC with a cable	Standalone (no wires, less powerful processor) + option to wirelessly stream to a PC	Tethered (wired to your PC, more powerful, can run larger models)	Tethered (wired to your PC, more powerful, can run larger models)	Tethered (wired to your PC, more powerful, can run larger models)	Tethered (wired to your PC, more powerful, can run larger models)
Price	\$299	 \$699	\$599	\$999	\$1399  \$1599	\$1199  \$1399
Summary	A great standalone headset for personal or business use. What you lose in processing power you gain in easy setup and freedom of movement. AirLink and the Link cable makes this a great option for running larger models as well.	A fantastic Enterprise standalone (or optional PC-streaming) headset focused on privacy and control, with ability to deploy software through Multiple Device Managers.	An affordable, high-res, tethered headset for running large models from your PC.	A top-of-the-line gaming headset. Base stations and wires require more setup and configuration, but create a smooth and powerful experience in-headset.	A top-of-the-line gaming headset. Base stations and wires require more setup and configuration, but create a smooth and powerful experience in-headset.	An older but still powerful gaming headset. Base stations and wires require more setup and configuration, but create a smooth and powerful experience in-headset.

One key difference between previous iterations of VR hardware is whether the headset is entirely self-contained or the system must be tethered to a PC to function. The Meta Quest 2 (Oculus) offers a stand-alone headset while some of the most popular precursors, such as the Valve Index and Vive Pro, must be tethered to a PC.

¹⁰¹ Source: “What VR Headsets Are Supported in the Wild?,” Wild, August 2, 2022, <https://thewild.com/help/vr-headset-support>. As of this writing, Meta, Apple, and several other companies have released newer versions of their headsets.

C. THE METAVERSE

The metaverse, owned by Meta—formerly Facebook—has been hailed as the “future of connection.”¹⁰² Although that may be a bold statement and hotly contested, the mass-market implementation of VR is revolutionary.¹⁰³ Arguably, the technological infrastructure for the metaverse is not there quite yet, so the technology’s capabilities as of this writing are merely a preview of the potential.¹⁰⁴ Nevertheless, the metaverse as it exists is powerful and deserving of recognition. As discussed in this thesis, the metaverse refers to Meta’s metaverse and the headsets used to access it, including the Meta Quest, Meta Quest 2, and the Meta Quest Pro, formerly Oculus, headsets. These headsets allow users to access the metaverse, a massive open-world environment that hosts games, social communities, and even virtual workspaces.¹⁰⁵ Games are available for free and purchase, and some applications offer in-game economics. Most popular games are single-player experiences, but many also have multiplayer options. VR games run the gamut of action-adventure style games, sports games, story and RP games, and even ones that focus on art and creativity.

The Meta Quest headset systems’ ease of use, design, and mass-market availability lends the system the potential for tremendous impact on future VR technologies. The headset is wireless, allowing users to move freely within a predefined space, with a built-in audio and microphone system that creates an authentic all-in-one experience. The system has been pioneered as easy to use, with intuitive controls and motion tracking.

Examples of popular VR games on the system include Beat Saber and Elite Dangerous. Beat Saber, a widely popular VR game, allows players to use their controls as

¹⁰² “About the Metaverse,” Meta, accessed January 26, 2023, <https://about.meta.com/metaverse/>.

¹⁰³ Karissa Bell, “How Meta Flunked Its First Year as a Metaverse Company,” Engadget, December 20, 2022, <https://www.engadget.com/how-meta-flunked-its-first-year-as-a-metaverse-company-150049067.html>.

¹⁰⁴ Avi Hadad, “Just like IRL, the Metaverse Requires Infrastructure. We Don’t Have It Yet,” TechCrunch, April 4, 2022, <https://techcrunch.com/2022/04/04/just-like-irl-the-metaverse-requires-infrastructure-we-dont-have-it-yet/>.

¹⁰⁵ “What Is the Metaverse?,” Meta, accessed January 26, 2023, <https://about.meta.com/what-is-the-metaverse/>.

light sabers, slashing at cubes that fly toward the user. The cubes follow the beat of popular songs, allowing for a hypnotic full-body musical experience (see Figure 7). Another popular game, Elite Dangerous, is a flight simulator set in the Milky Way galaxy, allowing players to explore a massive open world in outer space (see Figure 8).



Figure 7. Beat Saber VR Game.¹⁰⁶

¹⁰⁶ Source: Ian Hamilton, “Facebook: Beat Saber ‘Saved’ Oculus Quests,” Upload VR, March 29, 2021, <https://uploadvr.com/facebook-beat-saber-imu/>.



Figure 8. Elite Dangerous VR Gameplay.¹⁰⁷

A variety of third-party apps are accessible within the metaverse, creating a vulnerability for Meta, as these spaces are unregulated, and Meta cannot moderate the content and users of these spaces effectively.¹⁰⁸ Apps like VRChat and RecRoom allow for socialization with other users, real-time chat features, and even mini games within the apps that encourage social interaction.

Polls indicate significant growth for the metaverse, with adoption in the consumer market in the next five to ten years. Figure 9 illustrates projections of time spent in the metaverse by generation in the next five years. Like many new technologies, there are plenty of naysayers, but the future remains bright.¹⁰⁹ Thus, the metaverse will enhance human connections but present risks for homeland security practitioners. These risks,

¹⁰⁷ Source: “Elite Dangerous,” Steam, accessed March 3, 2023, https://store.steampowered.com/app/359320/Elite_Dangerous/.

¹⁰⁸ Emily Baker-White, “Meta Wouldn’t Tell Us How It Enforces Its Rules in VR, so We Ran a Test to Find Out,” BuzzFeed News, February 11, 2022, <https://www.buzzfeednews.com/article/emilybakerwhite/meta-facebook-horizon-vr-content-rules-test>.

¹⁰⁹ Janna Anderson and Lee Rainie, *The Metaverse in 2040* (New York: Pew Research Center, 2022), <https://www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040/>.

though not unlike existing online threats, become more foreboding when coupled with VR's ability to bridge the gap between the real and the imaginary.

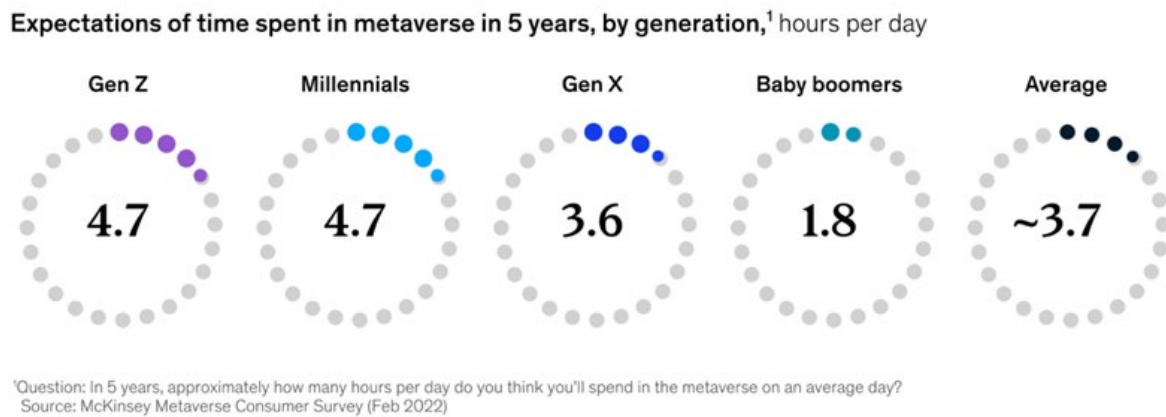


Figure 9. Projected Time Spent in the Metaverse by Generation in Five Years.¹¹⁰

¹¹⁰ Source: "Let's Meet in the Metaverse," McKinsey & Company, August 4, 2022, <https://www.mckinsey.com/featured-insights/sustainable-inclusive-growth/chart-of-the-day/lets-meet-in-the-metaverse>.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CRIMINAL ACTIVITIES WITHIN THE METAVERSE

Many types of criminal activity could occur within the metaverse, but this chapter focuses on extremism, crimes against children, and financial crimes. This chapter emphasizes the presence of criminal activity within the metaverse and its implications for homeland security experts, law enforcement, and policymakers.

Extremist and terrorist groups use social media for recruitment and communication.¹¹¹ When online gaming and social media merged into a more cohesive experience, it was not long before intelligence officials and law enforcement saw these platforms used for nefarious purposes.¹¹² Such risks are as prevalent in virtual environments as they are in other online spaces. Still, the novelty of these virtual spaces differentiates them from previous threats. Some dangers include extremist content on private servers, child exploitation, and financial crimes.¹¹³ VR environments, when coupled with sandbox worlds, accommodate user-created content on private or undetectable servers. Combined with the immersive nature of the metaverse and the ability to socialize anonymously, these vulnerabilities come into focus.

Each platform is responsible for its content moderation policies, and each app within the platform must establish policies regarding content, terms of use, and other governing strategies. The dissonance between the policies of tech giants, individual apps, and games enables prohibited content to slip through the cracks more easily, but gaming

¹¹¹ *Radicalization: Social Media and the Rise of Terrorism: Hearing before the Subcommittee on National Security of the Committee on Oversight and Government Reform, House of Representatives*, 114th Cong. (2015), <https://www.govinfo.gov/content/pkg/CHRG-114hhrg97977/html/CHRG-114hhrg97977.htm>.

¹¹² Jason Boone, *Criminal Use of Social Media* (Fairmont, WV: National White Collar Crime Center, 2011), <https://vrnclearinghousefiles.blob.core.windows.net/documents/Criminal%20Use%20of%20Social%20Media.pdf>.

¹¹³ Council of the European Union, “Online Gaming in the Context of the Fight against Terrorism” (official memorandum, Brussels: Council of the European Union, 2020), <https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf>.

companies are not wholly to blame. Regulating VR spaces is especially tricky because of the user-generated nature of many apps and social spaces.¹¹⁴

When addressing internet and virtual crimes, law enforcement must understand which laws apply in online investigations, particularly to companies that own these virtual technologies. Only two federal laws regulate big tech giants; the first concerns the privacy of minors operating on the internet, and the other focuses on removing content linked to sex trafficking. No federal regulations or laws govern extremist content, violent hate speech, or mis-, dis-, or mal-information.¹¹⁵ These limitations make it particularly difficult for law enforcement to address crime in the metaverse.

Criminal activity and threats in the metaverse may have different approaches; however, this thesis focuses on three overarching threats and some of the difficulties in combating them in the metaverse: crimes against children, financial crimes, and terrorism. All of them have well-established criminal networks on the internet. Thus, their transference to the metaverse is not so much an if but a when and how.¹¹⁶ These crimes can occur within the metaverse in different ways, but a lack of legislation expressly prohibiting these activities in the metaverse remains a significant barrier. Additional complications involve law enforcement resources when investigating digital crimes, jurisdictional challenges, and the law enforcement community's general lack of understanding of the metaverse. This chapter illustrates how common online threats infiltrate the metaverse.

¹¹⁴ Elizabeth Yin, Mary Moynihan, and Alexandra Walsh, "Regulating the Metaverse," *Regulatory Review*, January 7, 2023, <https://www.theregreview.org/2023/01/07/saturday-seminar-regulating-the-metaverse/>.

¹¹⁵ Cecilia Kang, "As Europe Approves New Tech Laws, the U.S. Falls Further Behind," *New York Times*, April 22, 2022, <https://www.nytimes.com/2022/04/22/technology/tech-regulation-europe-us.html>; "Hate Speech and Hate Crime," American Library Association, accessed January 24, 2023, <https://www.ala.org/advocacy/intfreedom/hate>.

¹¹⁶ Nitin Kumar, "Six Unaddressed Legal Concerns for the Metaverse," *Forbes*, February 17, 2022, <https://www.forbes.com/sites/forbestechcouncil/2022/02/17/six-unaddressed-legal-concerns-for-the-metaverse/>.

A. CRIMES AGAINST CHILDREN

The diversity of online gaming platforms offers many benefits, but such widespread use also carries great risk. Many councils have created policies on the safety of online gaming and offered recommendations for protecting oneself online, chiefly guiding parents of minor children who use these platforms.¹¹⁷ The metaverse and other VR platforms have quickly become buzzwords for internet safety and privacy advocates. The Meta Quest headset is heavily marketed to individuals participating in online gaming who seek a more immersive experience. Considering the technical aspects of using the headset, it is difficult for parents and guardians to supervise children using the technology. Barring a screencast of the content to a television, thus allowing an audience to see what a user is experiencing, it is challenging to strictly control a child's movements while using the headset or keep track of the child's interactions. This problem becomes even more complex when apps allow users to mask their names, ages, and appearances using avatars.¹¹⁸ Many apps and games allow users to design more than one fully customizable avatar that they can display in the virtual world. These features enable adults to appear as children and vice versa, with little recourse.

Regarding child safety within the metaverse, one potential option is regulating technology companies themselves. Such a prospect would be complicated by age-verification technology, data privacy considerations, and the retention and massive scale to which it would apply. While various councils have focused on the safety of children who operate in VR environments, this goal remains difficult due to the newness of the technology. Many apps and games have specific terms of service that specify age limits and other guidelines, but they are challenging to enforce.

When using VR headsets, minor children can easily access spaces not intended for them. The proximity to another avatar in some virtual spaces allows users to communicate

¹¹⁷ "Virtual Reality and Child Safety," Children's Society, March 3, 2023, <https://www.childrensociety.org.uk/what-we-do/blogs/virtual-reality-and-child-safety>.

¹¹⁸ Ben Chester Cheong, "Avatars in the Metaverse: Potential Legal Issues and Remedies," *International Cybersecurity Law Review* 3, no. 2 (2022): 467–94, <https://doi.org/10.1365/s43439-022-00056-9>.

verbally in near real-time as opposed to via text in traditional chat rooms. Often, avatars that appear to represent adults are voiced by children. This situation puts children at significant risk of being exposed to inappropriate online content, particularly when they are interacting in spaces designed for users over the age of 18. Although designed for adults, these spaces often lack the moderation or control to prevent children from gaining access to them. A simple age checkbox to self-verify is not enough to prevent minors from gaining access to content that could be potentially harmful to them. This vulnerability also highlights the ability of individuals who wish to cause harm to children. It is widely known that children use VR apps, typically unsupervised—as highlighted in numerous app reviews in the Meta Store—which allows individuals who wish to target children to identify them easily and attempt to exploit them.¹¹⁹ In one case, a 13-year-old girl from Utah had been communicating with a 25-year-old man for over a month using a Meta headset and convinced to meet him in person. The teen was missing for two days before police located her with the man; he had traveled with her to Wyoming.¹²⁰ This sobering example shows how quickly crimes in the metaverse can bleed over to the real world.

In conjunction with the BBC, the National Society for the Prevention of Cruelty to Children (NSPCC) investigated how VR worlds, especially those in the metaverse, can be dangerous to children. The NSPCC warned that some metaverse apps are “dangerous by design.”¹²¹ A BBC researcher posing as a minor female in certain apps witnessed multiple concerning behaviors, sexual material, threats of rape, and even blatant racism.¹²² These risks are not unique to just one app within the metaverse. The BBC researcher gained access

¹¹⁹ Callum Hood, “New Research Shows Metaverse Is Not Safe for Kids,” Center for Countering Digital Hate, December 19, 2021, <https://counterhate.com/blog/new-research-shows-metaverse-is-not-safe-for-kids/>.

¹²⁰ Kiah Armstrong and Ryan Bittan, “Metaverse Kidnapping: Missing Teen Found with Man She Met through Oculus Meta Program, Police Say,” FOX8 WGHP, March 12, 2022, <https://myfox8.com/news/crime/metaverse-kidnapping-missing-teen-found-with-man-she-met-through-oculus-meta-program-police-say/>.

¹²¹ Ali Shutler, “Some Metaverse Apps Are ‘Dangerous by Design’ Claims Children’s Charity,” NME, February 23, 2022, <https://www.nme.com/news/gaming-news/some-metaverse-apps-are-dangerous-by-design-claims-childrens-charity-3168044>.

¹²² Igor Bonifacic, “Investigation of VRChat Finds Rampant Child Grooming and Other Safety Issues,” Engadget, February 23, 2022, <https://www.engadget.com/bbc-vrchat-child-safety-report-193124305.html>.

to virtual strip clubs, where avatars simulated sex acts and promoted other illicit activities (see Figure 10).



Figure 10. A Virtual Strip Club.¹²³

There is a significant lack of oversight within many of these apps and platforms within the metaverse. Threats of rape, sexual assault, and other crimes against people are not limited to children. Often, a user appearing as a female avatar is enough on its own to garner harassment from other users.¹²⁴ At some point, action must be taken to define what is illegal and what is not in the metaverse. According to the European Union Agency for Law Enforcement Cooperation,

These kinds of virtual experiences pose serious questions about the applicability of current legislation. Rape requires physical contact, while by definition, an avatar is virtual. However, as the embodied internet is one of the ways of describing the metaverse, one can imagine that, as the technology gets more sophisticated, this crude delineation between physical and virtual will become increasingly problematic. As these experiences

¹²³ Source: Crawford and Smith, “Metaverse App Allows Kids into Virtual Strip Clubs.”

¹²⁴ Basu, “The Metaverse Has a Groping Problem Already.”

become more embodied and start to feel more real, we will have to decide at which point virtual experiences will be equally impactful as those of the physical realm. It will be important to have a clear idea of what is to be considered criminal behavior in the metaverse and to have matching laws to provide the means to prosecute these transgressions.¹²⁵

Law enforcement has long struggled with crimes against children on Meta's various platforms, and the metaverse will likely be no different. The potential crimes against children, harassment, and even sexual assault can have a more severe impact on victims due to the immersiveness of the technology, especially given the haptic feedback of the headset and related accessories. Crime data suggest that criminals will use new platforms as they have previous ones. As the National Center on Sexual Exploitation states, "Meta owns Facebook, Instagram, and WhatsApp: all platforms that are consistently noted by researchers, survivors, and law enforcement among the top platforms for a host of crimes including grooming, child sexual abuse materials, and sex trafficking."¹²⁶

B. FINANCIAL CRIMES

VR can also be used to facilitate financial crimes, from simple internet-based scams and fraud to nefarious financial crimes, including funding terrorist groups and nation-state actors.¹²⁷ The European Union Agency for Law Enforcement Cooperation highlights the importance of addressing financial crimes in the metaverse,

The more one learns about metaverse plans from major players like Epic Games and Meta, the more it seems that anti-money laundering (AML) and know your customer (KYC) protections will be as important as they are in the real world. In a space populated by virtual businesses, selling virtual goods to avatars will require virtual money. This provides opportunities to transfer money across borders in a more difficult way for the authorities to monitor.¹²⁸

¹²⁵ European Union Agency for Law Enforcement Cooperation, *Policing in the Metaverse*, 17.

¹²⁶ "The Dirty Dozen List: Meta," National Center on Sexual Exploitation, accessed January 24, 2023, <https://endsexualexploitation.org/meta/>.

¹²⁷ European Union Agency for Law Enforcement Cooperation, *Policing in the Metaverse*.

¹²⁸ European Union Agency for Law Enforcement Cooperation.

The metaverse uses various cryptocurrencies and traditional currencies to facilitate peer-to-peer commerce and interactions. Cryptocurrencies are digital assets that are a version of a decentralized currency. They can be highly volatile, anonymized, and seemingly endless in supply.¹²⁹ Cryptocurrencies are already used in money laundering schemes, and the anonymous nature of these transactions already makes it difficult for law enforcement to keep up with nefarious actors; combine these challenges with the new and misunderstood technology of the metaverse, and law enforcement is facing an uphill battle in understanding and combating illicit financial activities in the metaverse.¹³⁰

C. TERRORISM

As the technologies available to users have expanded, so has the ability of terrorist organizations to recruit new members and plan future attacks. Historically, online spaces have facilitated radicalization, recruitment, and retention of individuals to extremist and terrorist ideologies.¹³¹ The ability to remain anonymous online, specifically within the metaverse, presents the opportunity to plan, prepare, and rehearse a terrorist attack or other mass-casualty events without being detected by law enforcement. This hidden factor becomes even more significant when private gaming servers become part of the metaverse environment. These plans and preparations can represent anything: a reenacted 9/11, school shooting-themed games, and other mass attacks.¹³² In the virtual realm, where a user is limited only by one's imagination, with modified controllers allowing one to practice using firearms or flying a plane, the magnitude becomes even more impactful (see Figure 11).¹³³

¹²⁹ Nicole Lapin, "Explaining Crypto's Volatility," *Forbes*, December 23, 2021, <https://www.forbes.com/sites/nicolelapin/2021/12/23/explaining-cryptos-volatility/>.

¹³⁰ Jeremy Roebuck, "Philly Feds Help Dismantle Popular Crypto Money-Laundering Site Responsible for Cleaning \$3 Billion in Illicit Funds," *Philadelphia Inquirer*, March 15, 2023, <https://www.inquirer.com/news/chip-mixer-crypto-bitcoin-seized-ming-quoc-nguyen-charges-20230315.html>.

¹³¹ Rosanna E. Guadagno et al., "Social Influence in the Online Recruitment of Terrorists and Terrorist Sympathizers: Implications for Social Psychology Research," *Revue internationale de psychologie sociale* [International journal of social psychology] 23, no. 1 (2010): 25–56, <https://www.cairn.info/revue-internationale-de-psychologie-sociale-2010-1-page-25.htm>.

¹³² Troughton, "Roblox Is Cracking Down on Players Recreating School Shootings."

¹³³ Farivar, "Extremists Creep into Roblox."

This ability to re-create a terrorist attack while remaining undetected presents a clear threat to homeland security.



Figure 11. VR Gun Stock Accessories.¹³⁴

Another risk is the user's perceived immersion in the metaverse. It becomes easier to manipulate people and recruit them to a potentially harmful ideology because they feel as though they are physically in the same environment. Individuals are more susceptible to being recruited to a violent ideology if they feel they are physically engaging with their recruiters.¹³⁵ This risk is significant because it can be challenging to combat radicalization when no one knows it is happening. Terrorists frequently use the internet and other online spaces to recruit and radicalize individuals to extremist ideologies. The internet allows for such vast communication and sharing of ideas that one may communicate with people thousands of miles away in just seconds.

Terrorists could also use the metaverse to plan and coordinate attacks in the real world without being detected by traditional means. The ability to share propaganda and

¹³⁴ Source: "VR Gun Stocks," Olen VR, accessed March 3, 2023, <https://www.olenvr.com/vr-gun-stocks>.

¹³⁵ Katelyn Ferguson, Moon Jung Kim, and Martyna Dobrowolska, "The Role of Video Games and Online Platforms in Terrorist Radicalization and Recruitment," Counterterrorism Group, June 17, 2021, <https://www.counterterrorismgroup.com/post/the-role-of-video-games-and-online-platforms-in-terrorist-radicalization-and-recruitment>.

ideologies without consequence is a lucrative tactic, and the financial component of the metaverse, particularly with untraceable currencies, creates an even more significant vulnerability.¹³⁶ Untraceable currencies within the metaverse would be a boon for terrorist financing operations.

D. CONCLUSION

The metaverse provides many of the opportunities that the internet does, but with a significantly more immersive experience. Online gaming, which has historically offered users an engaging social experience, has slowly transitioned toward facilitating criminal activity; thus, the homeland security enterprise can expect the same for VR applications.

¹³⁶ Jeter and Taylor, “Terrorist Presence in Virtual Worlds.”

THIS PAGE INTENTIONALLY LEFT BLANK

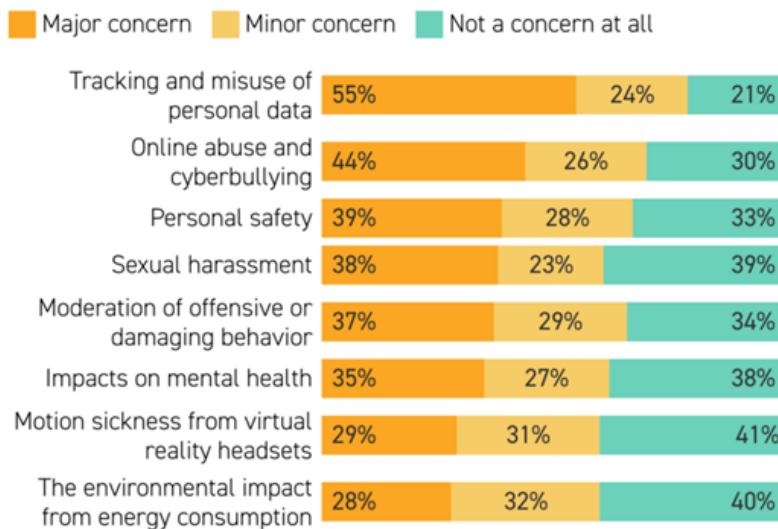
V. IMPLICATIONS FOR HOMELAND SECURITY

A. DATA PRIVACY AND ENCRYPTION

Privacy concerns and the metaverse may be viewed through multiple lenses; concerns for the broader homeland security enterprise and the metaverse are intertwined. As the metaverse becomes more popular, some risks accompany Meta’s collection and sale of personal data to third parties (see Figure 12). Moreover, bad actors may try to exploit such vulnerabilities to privacy.

Potential metaverse users worry about data, abuse

How much of a concern is each topic in using the metaverse?



Percentage of adults polled by Morning Consult. Poll in field March 3-5, 2022, with a 1 percent margin of error.

Source: Morning Consult
Derek Robertson / POLITICO

Figure 12. Metaverse Safety Concerns from 2022 Politico Poll.¹³⁷

¹³⁷ Source: Derek Robertson, “Crimefighting in the Metaverse,” Politico, April 13, 2022, <https://politi.co/3EanPxP>.

In VR apps, collecting information about another person’s avatar, account, and activities in the metaverse is relatively simple and can be done without the individual’s knowledge or consent. Sometimes, an individual can be tracked from app to app within the metaverse and other online spaces.¹³⁸ Data privacy is not a new concern for the American public when interacting in online spaces, nor is it for Congress and those who seek to harness the unchecked powers of the big tech industry and the data collected on users of online spaces.¹³⁹

The metaverse and the Meta headset will give Meta critical user data, including biometric data, eye/gaze tracking, pupil dilation, and other sensitive information about its users.¹⁴⁰ The Meta headset can also scan a user’s space and identify objects in the room.¹⁴¹ Meta recently added the ability for users to connect their health apps via Apple and Android devices, allowing users to pair Bluetooth heartrate monitors, active calories burned, and other exercise stats. Such data will not be shared automatically with Meta, but a user may choose to sync another device with one’s headset after agreeing to the privacy terms for both the device and Meta.¹⁴² The users, while consenting to share these data with big tech when purchasing and using the headset, may not even realize the sheer amount of information collected about them and their lifestyles.

Some experts have expressed concern over the data encryption technology of the Facebook Messenger app for the Meta headset. While data encryption for the Messenger app in the headset is the same as for other devices, the privacy terms for the Meta headset, which are distinct from one’s Facebook account, do not explain whether Meta can sell the

¹³⁸ European Union Agency for Law Enforcement Cooperation, *Policing in the Metaverse*.

¹³⁹ “Transcript: Innovation, Data, and Commerce Subcommittee Hearing on Data Privacy,” Tech Policy Press, March 2, 2023, <https://techpolicy.press/transcript-innovation-data-and-commerce-subcommittee-hearing-on-data-privacy/>.

¹⁴⁰ Girard Kelly et al., *Privacy of Virtual Reality: Our Future in the Metaverse and Beyond* (San Francisco: Common Sense Media, 2022), <https://www.common sense media.org/sites/default/files/research/report/privacy-of-virtual-reality-our-future-in-the-metaverse-and-beyond.pdf>.

¹⁴¹ Kelly et al.

¹⁴² Victoria Song, “Meta Quest Users Can Now Track Their Heart Rate in VR Workouts,” Verge, January 11, 2023, <https://www.theverge.com/2023/1/11/23550611/meta-quest-heart-rate-health-connect-android>.

data it collects. Nevertheless, the terms allow targeted advertising while using the headset. Notably, the data collected could comprise anything, from the device ID, to cookies, to any information submitted to third-party sites within the headset.

The following information may be collected about a user, according to the Meta headset's privacy policy:

- User's name, email address, phone number, and location information;
- recordings and transcripts of a user's voice interactions; and
- biometric information about the users' environment, physical movements, and dimensions when they use a Meta device.¹⁴³

B. CONTENT MODERATION

Content moderation is a complex issue given its implications for governmental censorship and First Amendment rights. An equally important and often overlooked issue involves the individuals responsible for content moderation on online social media sites and spaces.¹⁴⁴ The individuals who serve as content moderators are repeatedly exposed to horrific material, and the mental and physical well-being of these employees has been richly documented.¹⁴⁵ Content moderation in the metaverse presents many of the same challenges as that on other platforms; however, immersion elevates the concerns to a higher level.

Beyond content moderation issues, regulating the behavior of those in the metaverse is an overriding challenge. Distinct from existing online spaces, the metaverse

¹⁴³ "Common Sense Privacy Standard Privacy Report for Oculus," Common Sense Media, December 6, 2022, <https://privacy.commonsense.org/privacy-report/Oculus>.

¹⁴⁴ Brandon Dang, Martin J. Riedl, and Matthew Lease, "But Who Protects the Moderators? The Case of Crowdsourced Image Moderation," arXiv, 2020, <https://doi.org/10.48550/arXiv.1804.10999>.

¹⁴⁵ Miriah Steiger et al., "The Psychological Well-Being of Content Moderators: The Emotional Labor of Commercial Moderation and Avenues for Improving Support," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (New York: Association for Computing Machinery, 2021), 1–14, <https://doi.org/10.1145/3411764.3445092>.

puts the spotlight on the behavior of virtually represented individuals.¹⁴⁶ Meta struggles to successfully moderate its current non-VR platform, so effectively moderating an even more significant, more complex environment will likely be challenging. The reporting functions that do exist are often ignored, according to experts, and the reporting mechanisms for various Meta platforms often lack authority and responsiveness.¹⁴⁷

C. MONITORING AND SURVEILLANCE

To effectively moderate the metaverse, whether behavior or content, someone must monitor the virtual realm either live or on a delay—but each has unique challenges. Users are naturally hesitant to be monitored by any governmental entity in a space free from such supervision except in the most stringent spaces. Meta already monitors users and collects their data for marketing and sales, but whether the company is doing so to protect the end user remains to be seen.¹⁴⁸ Law enforcement needs to understand the metaverse and virtual spaces to grasp the potential homeland security implications of such a new technology.

D. CIVIL LIBERTIES

The use of virtual worlds such as the metaverse by government entities presents the concern of government overreach and the subtle erosion of civil rights and civil liberties. The constitutionality of such surveillance is likely to be hotly debated, like the government surveillance of other social media platforms. The mere immersiveness of the metaverse makes it much more difficult for governments to passively observe open-source intelligence and social media, as there must be a participatory end user. Due to the varied capabilities of U.S. law enforcement agencies, it is difficult to ascertain whether any agencies are exploiting the metaverse to track criminal activity. Interpol has begun training

¹⁴⁶ Aaron Mak, “I Was a Bouncer in the Metaverse,” *Slate*, May 9, 2022, <https://slate.com/technology/2022/05/metaverse-content-moderation-virtual-reality-bouncers.html>.

¹⁴⁷ Baker-White, “Meta Wouldn’t Tell Us How It Enforces Its Rules.”

¹⁴⁸ “To Address Emerging Privacy Issues, Congress Should Consider Comprehensive Legislation,” Government Accountability Office, September 13, 2022, <https://www.gao.gov/blog/address-emerging-privacy-issues-congress-should-consider-comprehensive-legislation>.

officers on a variety of apps in the metaverse but acknowledges that “sometimes lawmakers, police, and our societies are running a little bit behind.”¹⁴⁹

E. ANONYMITY

The Meta Quest headset, used to access the metaverse, offers two forms of identity management. One links a user’s Facebook account directly to the headset, thus allowing a more connected social experience. Second, for those without a Facebook account, they must create a Meta account that allows digital purchases and is separate from any existing social media presence. The same procedures apply if individuals do not want to link their Facebook accounts to the headset. Theoretically, an individual could create a false identity on Facebook and use that profile in the metaverse to misrepresent one’s identity.¹⁵⁰ Lax terms of service on various platforms, combined with the lack of oversight, allow for the proliferation of dummy accounts. They can be created and burned faster than the site can take them down, and in most cases, account creation is free.

Virtual private networks (VPNs) allow individuals to mask their IP addresses when accessing the internet. Briefly, a user accesses the VPN from one’s internet service provider. Through the service, the user is rerouted to appear as though coming from a different geographical location. Using a VPN or other identity concealment technique is not inherently nefarious, but bad actors may use such tools unethically to facilitate criminal activity.

Blockchain technology forms the foundation of part of the metaverse. Decentraland and The Sandbox, apps hosted by the decentralized autonomous realm of the metaverse, are not games but have robust economies. As representations of the real world, they allow users to do anything virtually that they could do physically, such as go shopping, buy

¹⁴⁹ Jamie Harris, “Meta Police: Inside Interpol’s Secret Virtual HQ as Cops Plan to Hunt Criminals in the Metaverse,” *U.S. Sun*, February 6, 2023, <https://www.the-sun.com/tech/7319286/interpol-metaverse-crime-police/>.

¹⁵⁰ Davy Smith, “Multiple Identities, Security, and the Growth of the Metaverse,” *Maddyness*, December 5, 2022, <https://www.maddyness.com/uk/2022/12/05/multiple-identities-security-and-the-growth-of-the-metaverse/>.

property, or go to a virtual concert, strip club, or a casino. Decentraland, accessible through the Meta headset, is a third-party app because Meta does not own it.¹⁵¹

The use and conversion of cryptocurrency in virtual spaces supercharges the opportunity for committing crimes, profiting from them, and staying out of law enforcement's reach. Cryptocurrency can be a relatively anonymous means of buying and selling goods—it is particularly desirable when one wants to conceal an online identity from others or purchase illicit goods.¹⁵² Privacy-focused individuals may prefer to use cryptocurrencies such as bitcoin and a wallet with a private key to buy and sell goods that transfer to the physical world. Some major real-world retailers are even beginning to accept cryptocurrency as a valid form of payment.

Some cryptocurrency is a volatile investment, though, as it is unregulated and unrecognized as currency by the government. The foundation of blockchain technology and the primary financial function of cryptocurrency within the metaverse allow users their preferred level of anonymity—depending on their internet savvy. If they choose, users may purchase a Meta headset with cash, use a VPN on a home network, create a false identity using Meta or Facebook, create an anonymous crypto wallet, and function entirely anonymously in the metaverse. Such anonymity would allow users to interact freely with other users with few consequences besides content violations that might result in an account ban or other measures taken by Meta's moderation team.

F. DECENTRALIZATION

This thesis focuses specifically on Meta's metaverse, a centralized VR space; however, the future of the metaverse and its representation bears discussion, too, because of the knotty problem of end-user-created content. The difference between a decentralized and a centralized metaverse lies in who holds power: "In a centralized Metaverse, users can freely create content or games, but ownership of those games is given to the entity

¹⁵¹ "Decentraland VR," SideQuest, accessed April 17, 2023, <https://sidequestvr.com/app/11626/decentraland-vr>.

¹⁵² Elizabeth Howcroft, "Crypto Crime Hits Record \$20 Bln in 2022, Report Says," Reuters, January 12, 2023, <https://www.reuters.com/business/finance/crypto-crime-hits-record-20-bln-2022-report-says-2023-01-12/>.

behind that virtual world. In the case of a decentralized Metaverse, on the other hand, the content or games created there remain the property of the creator users.”¹⁵³ One significant benefit of decentralization for big tech is that the value of the platform derives from consumers and their data—user data become monetized. However, in a decentralized metaverse where users and products cross platforms while still maintaining control, the value shifts to the consumer. Rather than being monetized, the user controls that process.

As the metaverse becomes more sprawling and developed, it will increase the risk of criminal and terroristic activity. The anonymity of the metaverse will make it particularly difficult to track and identify illegal activity. The metaverse is an open marketplace for people to create and sell content and even design their own private spaces. As such, Meta owns the infrastructure of the metaverse, but it does not own or control the content created within. This dynamic creates potential problems for law enforcement in tracing an individual’s real-world identity during an investigation. There is no central point of control for law enforcement to rely on when criminal matters inevitably develop in the metaverse.

¹⁵³ Anna Cela, “Is the Structure of Metaverse Centralized or Decentralized?,” *TechStar* (blog), December 7, 2022, <https://www.techstar.it/en/blog/is-the-structure-of-metaverse-centralized-or-decentralized/>.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. SURVEY

The data collected from the metaverse user survey illustrate that the metaverse presents inherent risks to individuals and, more broadly, homeland security; Meta is not addressing the concerns, and these threats are likely far more extensive than realized due to the nature of the metaverse and its affiliated VR technologies.

A. METHODS

A survey was administered to gather qualitative data on user experiences within Meta's metaverse. The survey was administered via Qualtrics to participants at the Naval Postgraduate School and then to the general population via Amazon's Mechanical Turk (MTurk) with the Qualtrics link embedded. The survey garnered 405 total responses. Due to time constraints, the survey was open for a period of one month, from February 2023 to March 2023.

The survey responses collected through the Qualtrics platform were qualitative and involved users' first-hand accounts of their experiences within the metaverse. The survey asked users not to specify in which apps they experienced the behavior but merely to report what they had observed or experienced themselves. The survey, which targeted users of the metaverse through the Meta Quest headsets, aimed to establish a baseline of user experiences. The questions initially focused on the participants' use of Meta's metaverse—frequency; social interaction on the platform; and purpose, for example, social, professional, or other.

The survey was then divided into three major sections focusing on the experiences of the users with the metaverse. The first set of questions were not limited to Meta-owned applications but instead focused broadly on the entirety of users' experiences. The goal of this survey was to identify the frequency with which malicious activity occurred within the metaverse but went no further than that. The questions in the next sections focused on violations of the terms of service (TOS) for the platform and observations of explicit behavior or content violations. From that point, the survey focused on the three primary areas of discussion for this thesis: financial crimes, harassment and child exploitation, and

extremism. The questions then addressed whether any children in the household had unsupervised access to the Meta platform, whether being a victim of crime or harassment within the metaverse changed the users' perception of the technology, and whether it was important to address potential crime within the metaverse. See the Appendix for the survey questions and select responses.

B. SURVEY DATA

The quality of the survey data varied significantly in the responses received; many of the responses garnered from MTurk appeared to be bot-generated or were answered improperly. The few true responses illustrated that various illicit activities are occurring within the metaverse. This survey represented only a small percentage of users of the metaverse, suggesting the data underrepresent the true occurrence of these activities on the platform.

Overall, many of the responses indicated broad themes of malicious and harmful behavior. For example, the responses detailed individuals portraying avatars representing Adolf Hitler, the presence of unattended and unsupervised minors, the recruitment of players to extremist groups, and many other concerns discussed in this thesis. While the author acknowledges that the data set was relatively small, the findings point to significant issues likely occurring on a broader scale than this survey could capture. Figure 13 compiles all freeform responses in the user survey that detailed troubling scenarios encountered by users of the metaverse.

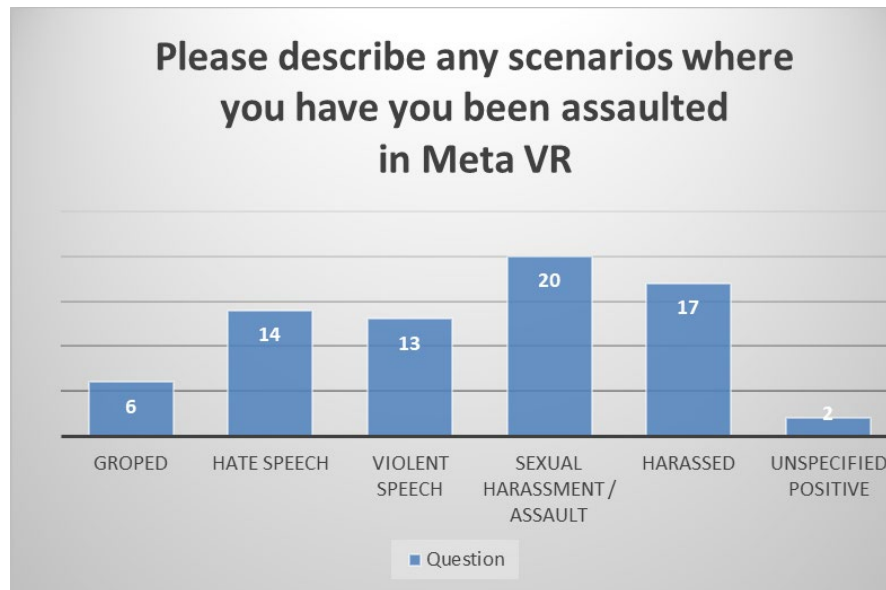


Figure 13. Accounts of Assault by Metaverse Users

Some of the most poignant responses to the survey questions follow. In answering the prompt “Please describe any scenarios where you have been assaulted in Meta VR,” the following response was collected:

In MetaVR, I have been harassed verbally and subjected to hateful speech. I have also been groped, and sexually assaulted. On one occasion, I was simulating a scenario in which I was playing a victim of a simulated rape. I was verbally harassed by the perpetrator, and I felt extremely uncomfortable and scared. I was also physically harassed with unwanted touches and was subjected to violent speech. This was a deeply traumatic experience for me, and it made me feel very uncomfortable in MetaVR.

As discussed earlier in this thesis, identity and alias accounts present an issue for users of the metaverse. One user, in response to the question addressing extremist content detailed the following:

I’ve encountered users wearing avatars of Adolf Hitler, Joseph Stalin, and Osama Bin Laden on separate occasions. The users otherwise acted normal, but they were intentionally trying to disrupt or break into others’ conversations to surprise/shock them as a “prank.” These users seemed to be in their early-mid teens (anecdotally, based on their voices).

Additional research discussed in the next chapter corroborates the presence of individuals exhibiting similar behaviors.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CENTER FOR COUNTERING DIGITAL HATE

The Center for Countering Digital Hate (CCDH) conducted similar research on the VRChat app in the metaverse. The data from its survey were reviewed and compared to the survey data derived for this thesis. The CCDH survey on VRChat experiences showed instances of concerning behaviors related to metaverse usage.

The research methods used by the CCDH team involved accessing virtual worlds through the VRChat app with the Meta Quest headset and capturing encounters with the built-in recording feature. Each world explored had multiple active sessions with a maximum number of users. In the case of one world, thousands of users were active at the same time, but each iteration could host a maximum of 18 users. Most of these worlds were publicly accessible, but there were some private, invite-only groups. The researchers reported policy violations to Meta using the reporting function and documented the incidents for their research. Data were collected between November 29, 2021, and December 19, 2022.¹⁵⁴

Accounts varied on whether users had reported other accounts for TOS violations, with responses indicating a range of reasons for reporting a fellow user. The CCDH process indicated that while researchers identified over 100 policy violations according to Meta's TOS, only 51 were reportable using the web-based platform.¹⁵⁵

The CCDH researchers accessed some of the most popular worlds in VRChat, including one that simulated a bar environment and one that mimicked a sex club. The data provided by the center cover approximately 11.5 hours spent in VRChat. As a comparison, VRChat boasts 19.6 million users and 2.4 million active users.¹⁵⁶ Playtime averages 63.9 hours for a user, so the data provided by center likely represent a minuscule portion of the content violations in this one app within the Meta's metaverse. Types of abuse that CCDH

¹⁵⁴ Hood, "New Research Shows Metaverse Is Not Safe for Kids."

¹⁵⁵ Hood.

¹⁵⁶ "VRChat Stats," PlayTracker, accessed February 27, 2023, <https://playtracker.net/insight/game/2704>.

researchers documented included bullying or harassment, hate speech, inappropriate behavior, inappropriate content, and encouraging harm. Further, the categories of abuse recorded included abuse, racism, homophobia, sexual content, transphobia, drugs, misogyny, child abuse, and rape (see Table 3).

Table 3. Content Violations Observed in VRChat by CCDH Researchers.¹⁵⁷

Category	Minors Present		
	Yes	Unknown	Grand Total
Abuse	5	4	9
Child Abuse	1	1	2
Drugs	1		1
Encouraging Harm	1	1	2
Extremism	1		1
Harassment	5	1	6
Holocaust Denial	1		1
Homophobia	4	8	12
Inappropriate Age	2		2
Misogyny		3	3
Racism	9	12	21
Rape	1	1	2
Sexual Content	33	4	37
Transphobia		1	1
Grand Total	64	36	100

CCDH researchers documented the presence of minors in VRChat, as well as the following:

¹⁵⁷ Adapted from Hood, “New Research Shows Metaverse Is Not Safe for Kids.”

- Nearly two-thirds of reports (64 percent) were for policy violations that took place in the presence of minors.
- A third of those (33 percent) involved users sharing or displaying sexual content in front of minors.
- Some users adopted avatars projecting graphic pornography that depicted minors across entire instances of VRChat.
- Researchers studying the most popular social app in Meta’s VR app store found that users, including minors, are exposed to abusive behavior every seven minutes.

Researchers also observed grooming behavior, racism, extremist content, and Meta TOS violations. Of the 100 reportable offenses documented, children were confirmed present in 64 incidents, and their presence was unknown in the other 36 incidents. These data further validate the original survey data collected as a part of this thesis, confirming the existence of malevolent behavior within the metaverse and emphasizing the need for the homeland security enterprise to take action.

Additionally, user reviews of the VRChat app were evaluated, and multiple content violations were detailed in such reviews. Due to the nature of the reviews, further context and information on whether the abuse was reported to Meta or any action was taken are unavailable (see Figure 14).

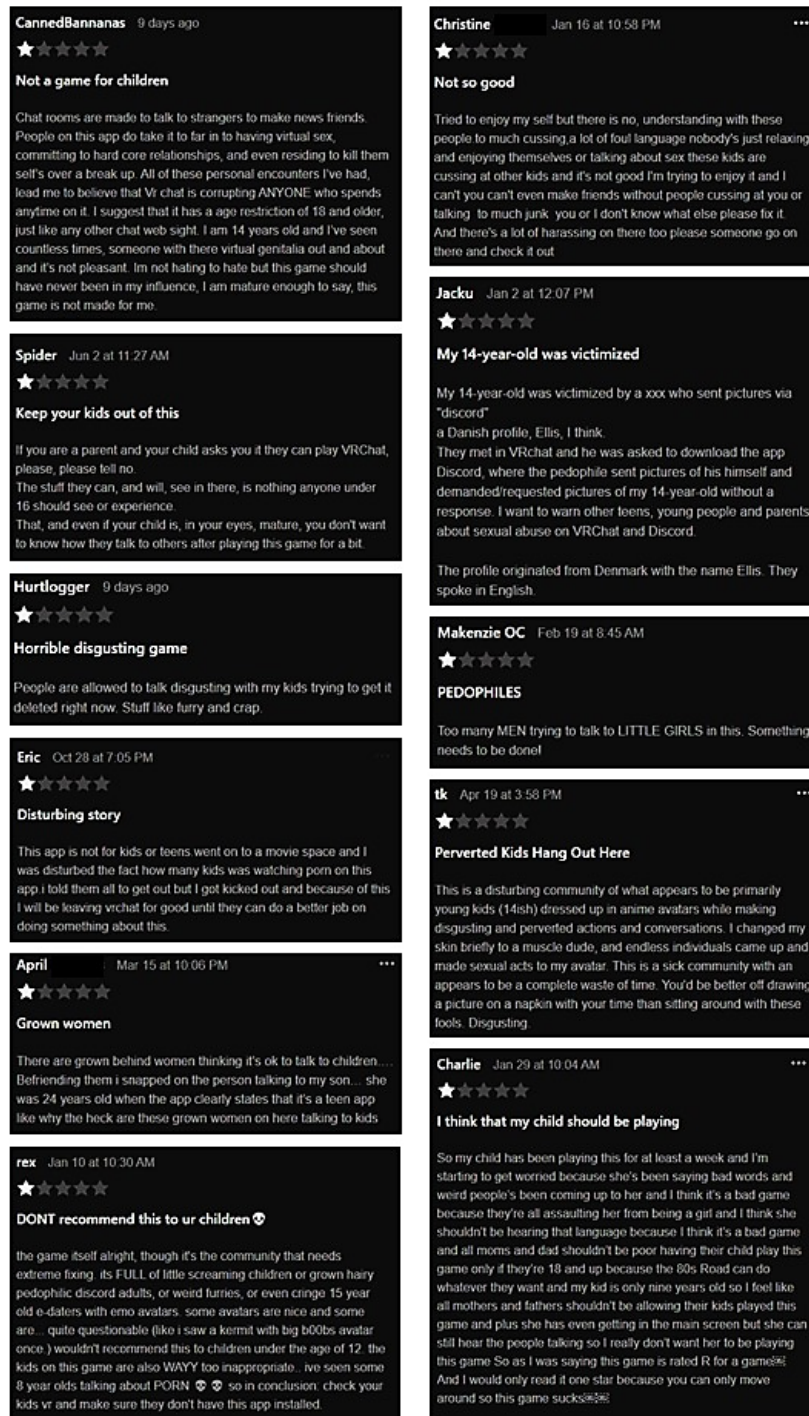


Figure 14. Disturbing Reviews of VRChat in the Meta Store.¹⁵⁸

¹⁵⁸ “VRChat: Reviews,” Meta Quest Apps & Games, accessed August 10, 2023, <https://www.oculus.com/experiences/quest/1856672347794301/>.

VIII. CONCLUSION

The metaverse presents an unprecedented opportunity for global technological innovation. There are benefits and drawbacks to the inevitable integration of the metaverse in our day-to-day lives. Society, individuals, governments, and the private sector must prepare to deal with the consequences if they are also to benefit from the metaverse.

There are problems with the metaverse, even in its early development, and they will not go away. They are not unlike the concerns, worries, and predicted problems surrounding other new technologies; the difference this time is how seamlessly these issues can permeate the real world and create unforeseen complications from a technology with no bounds. The National Center for Missing and Exploited Children received more than 29 million reports of child exploitation online in 2021. These numbers have grown every year since 2019.¹⁵⁹ The presence of financial crime online is well documented, with the FBI's Internet Crime Complaint Center receiving 800,944 reported complaints, with losses exceeding \$10 billion.¹⁶⁰ Extremism and terrorism, too, have an established presence in internet spaces, and the metaverse as well.

A. FINDINGS

The metaverse represents the future of human technological advancement in a way depicted only previously in works of science fiction. This thesis set out to educate the reader on the historical context of VR, explain the significance of new VR technology, and lay the groundwork for the study and research of Meta's metaverse. In doing so, the primary question this thesis sought to answer was what homeland security professionals need to consider in understanding potential malicious activity and threats affiliated with the increasing usage of the metaverse. This thesis sought to provide special attention to the ramifications of widespread accessibility of the metaverse for law enforcement and the

¹⁵⁹ "CyberTipline 2022 Report," National Center for Missing and Exploited Children, accessed April 18, 2023, <http://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.html>.

¹⁶⁰ "Internet Crime Complaint Center Releases 2022 Statistics," Federal Bureau of Investigation, Springfield Field Office, March 22, 2023, <https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics>.

Intelligence Community. In doing so, this research explored the prevalence of criminal and terroristic activity, including financial crimes and crimes against children, within the metaverse that will have real-world consequences for users.

Though limited in scope, the research from CCDH revealed numerous threats within Meta's metaverse and little recourse for the average user or law enforcement officer to combat them. As the metaverse becomes more robust, it will be necessary for law enforcement to understand virtual environments but also prepare to fight crime in a way that differs fundamentally from traditional law enforcement investigations. This exploration laid the foundation for future researchers into this realm, as the metaverse is a vast and immeasurable space undergoing constant evolution and change.

Users of the metaverse were surveyed to illustrate which nefarious activities are occurring on the platform. While the survey data were limited in scope, corroborating data from other researchers further validated that these threats are happening. However, there is little action in dealing with them, so they are likely to proliferate exponentially.

B. RECOMMENDATIONS

VR experts have established numerous potential issues and solutions regarding the metaverse and other VR platforms that need to be addressed before their widespread adoption. One solution places the onus on the platforms rather than a governmental regulatory body. This suggestion would sidestep some stickier issues in regulating an environment concerned with free speech. This option does, however, present the inherent risk of allowing big tech to self-police, something that has been tried in other iterations, albeit unsuccessfully. The other solution would be to impose a regulatory body over VR spaces, a massive undertaking that first involves gaining the understanding and buy-in of policymakers and industry experts; a problem must be demonstrated, and the solution must make sense without being too complicated or cost-prohibitive.

VR experts have emphasized concerns about the overall security of the metaverse, the widescale adoption of which presents a unique set of challenges. Various concerns have been raised and potential solutions offered to help make the metaverse a more secure space. The issues already present in online spaces, such as privacy concerns, data encryption,

content moderation, and government surveillance, are just as applicable to the metaverse, if not more so.¹⁶¹

1. International Cooperation

The metaverse offers a unique opportunity for international collaboration for users and those seeking to research and regulate the space. With the potential for users to become closer than ever despite the physical separation of continents, international collaboration becomes increasingly important from a regulatory perspective, especially if criminal or terrorism concerns affect the space. Themes worth addressing include intelligence, national security, and nation-state vulnerabilities to exploitation by bad actors, from a cyber security perspective. For example, many U.S. law enforcement agencies have transitioned to using VR simulations as part of routine training exercises, leaving their tactics, techniques, and procedures vulnerable to bad actors who may have a vested interest in disrupting their organizational functions.

2. A Multi-disciplinary Approach

Tech companies have faltered in confronting violent hate speech and extremism that presents a security threat on their platforms, including Meta's metaverse. Social media has permanently altered the course of humanity, likely in ways that society has yet to realize. One accepted truth is that social media and online communities provide a platform for the voiceless to be heard, galvanizing their ideas and beliefs and providing an echo chamber for their orations. Specific algorithms curate user experiences to boost engagement, strengthen connectivity, and maximize profits.¹⁶² These powerful algorithms can be used to share toxic and harmful beliefs, misinformation, and other nefarious ideas.¹⁶³

¹⁶¹ Sam Jungyun Choi et al., "Regulating the Metaverse in Europe," Covington Global Policy Watch, April 11, 2023, <https://www.globalpolicywatch.com/2023/04/regulating-the-metaverse-in-europe/>.

¹⁶² Zachary Laub, "Hate Speech on Social Media: Global Comparisons," Council on Foreign Relations, June 7, 2019, <https://www.cfr.org/backgrounder/hate-speech-social-media-global-comparisons>.

¹⁶³ Katherine J. Wu, "Radical Ideas Spread through Social Media. Are the Algorithms to Blame?," NOVA Next, March 28, 2019, <https://www.pbs.org/wgbh/nova/article/radical-ideas-social-media-algorithms/>.

A multi-disciplinary approach to combating threats within the metaverse and dangers presented by its widescale adoption is this author's recommended approach to the potential problems that arise from its commercial success. Ethical and moral responsibilities come with the release of such a robust technology and wide accessibility by consumers. Education, of course, on what the system is capable of and instruction on the lasting repercussions of its misuse are paramount.

3. Economics, Costs, and Regulation

The impact of establishing and imposing a regulatory body on the metaverse will likely be widespread, with concerns originating from privacy and civil liberties experts and technology companies themselves. Some considerations in such regulation include data privacy, content moderation, and the digital market. All are significant individually and deserve considerable attention to capture a holistic view of the situation.

The metaverse is estimated to become a \$783 billion market by 2024.¹⁶⁴ It is essential that the costs of implementing a policy initiative for the metaverse are not exclusively financial. It bears mentioning that there are other costs and burdens to consider, particularly when suggesting regulation of the internet, which is traditionally a space free from government control. There are concessions to be made in the name of safety and security, often in the form of privacy and anonymity. Whether the American people are ready to accept that kind of cost remains to be seen.

4. Potential Challenges

Significant barriers exist regarding the implementation of any metaverse policy—the most noteworthy being that the metaverse is still in its infancy, and convincing policymakers of its importance in the future may be difficult. Many discussions surrounding the metaverse are still hypothetical, and proactive policy regulation is a difficult sell, even to the most receptive of audiences. No legislation has yet regulated online content, particularly extremist content, violent hate speech, or mis-, dis-, or mal-

¹⁶⁴ “Metaverse May Be \$800 Billion Market, Next Tech Platform,” *Bloomberg Professional Services* (blog), December 1, 2021, <https://www.bloomberg.com/professional/blog/metaverse-may-be-800-billion-market-next-tech-platform/>.

information.¹⁶⁵ Civil rights and privacy advocates will likely raise additional concerns; they should be acknowledged and treated as valid.

There are numerous critical stakeholders of the metaverse, specifically when securing buy-in for policies to deal with these challenges. Potential stakeholders include academic researchers, the Cybersecurity and Infrastructure Security Agency under the Department of Homeland Security, the National Child Safety Council, National Fusion Center Association executives, lawmakers, and representatives from the tech industry, including the Ford Foundation. Getting buy-in from each of these stakeholders will require a dedicated component and must be accomplished before implementing any metaverse-specific regulation. Integral to the process are also members of the Intelligence Community, investigators, and members of law enforcement with experience investigating internet-based crimes.

Policy and regulatory success regarding the metaverse depends heavily on the commercial success of Meta's Quest platform. Competitors are offering VR headsets and platforms rivaling the existing infrastructure rather than incorporating them into Meta's existing architecture. Another consideration is the government's ability to broadly encourage competition between VR platforms without committing to the regulation or policing of one specific environment but focusing on the entire environment.

Provided that the projections for the commercial success of the metaverse are at least somewhat correct, with an estimated market value of nearly \$783 billion by 2024, ongoing educational campaigns, research, and a solid commitment to early-stage development initiatives are crucial.¹⁶⁶ Due to the newness of both the technology and mass-market adoption, the sustainment of any policy initiatives will depend heavily on the industry's ability to harness the momentum of the technology in the beginning stages.

¹⁶⁵ Kang, "As Europe Approves New Tech Laws, the U.S. Falls Further Behind."

¹⁶⁶ "Metaverse May Be \$800 Billion Market."

5. Can't We Just Work Together?

Due consideration should be given to the relationship between governmental entities and organizations closely intertwined with free speech, individual liberty, and technology. The metaverse represents an opportunity to incorporate a variety of internet safety council organizations, youth safety organizations, media literacy groups, the Intelligence Community, global stakeholders, and many more.

The European Commission is leading the global community in both regulating and policing the metaverse in a variety of ways. A fact sheet titled “A Europe Fit for the Digital Age” discusses some of the most important facets of the metaverse and the regulations and proposed policies that the European Commission is considering for the virtual realm.¹⁶⁷ Also included is a timeline, proposed costs, and benchmarks for success. Additionally, the European Commission has established goals for European citizens to become more digitally literate, clear communications on the importance of data privacy, an online presence, and an overall strategy for the future of technology and society for Europe. Finally, the European Commission is developing a multi-pronged approach for the metaverse, including the Digital Services Act, the Digital Markets Act, the European Digital Identity Act, and more.¹⁶⁸ In essence, these proposed strategies, policies, regulations, and educational campaigns are worth considering for adoption in the United States—as well as globally—as the metaverse and other technologies continue to develop and grow.

The overall recommendation for metaverse policy implementation is to devise a multifaceted approach, including safety councils, academic working groups, governmental input, and a significant educational component. The safety council should have comprehensive situational awareness of the happenings of the metaverse, something that can only be achieved with academic collaboration. Internal data awareness protocols and complete oversight should be provided by Congress, and the material produced should be

¹⁶⁷ “A Europe Fit for the Digital Age,” European Commission, accessed April 17, 2023, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en#.

¹⁶⁸ European Commission.

available to the public as much as possible. Annual reports and trend analyses, with considerations for stakeholders, policymakers, and lawmakers, will be essential in all phases of the initiative.¹⁶⁹ Additional recommendations include introducing a regulatory system and systematic audits to better enforce content moderation within big tech and social media companies.¹⁷⁰

C. FUTURE RESEARCH

The metaverse offers many opportunities, but without more significant research and enhanced collaboration between industries—homeland security, tech, and Meta—it may struggle to reach its full potential. I see a future of investment in the metaverse allowing for significant growth and opportunity, but concerns about its vulnerabilities are valid. This thesis addresses some of the most critical issues within the metaverse in hopes that future researchers and homeland security professionals will see the metaverse as a worthwhile investment opportunity that provides the chance for remarkable development if it is used correctly.

Opportunities for future research include the further exploration of criminal activity and extremist recruiting within the metaverse and other yet-developed VR spaces. Research should collect both quantitative and qualitative data and include reports from users of the metaverse platform, with surveys targeting larger sample sizes and questions inducing more in-depth responses. Finally, researchers might pose as individuals in the metaverse as those with CCDH did to capture first-hand experiences of nefarious activities in virtual spaces. Future research should also explore the many potential benefits of using the metaverse—communication; virtual workspaces; and healthcare, military, and law enforcement training scenarios all could be integrated into virtual environments to help the homeland security enterprise adapt to the constantly evolving threat stream that faces the global security community.

¹⁶⁹ Choi et al., “Regulating the Metaverse in Europe.”

¹⁷⁰ Choi et al.

This thesis sought to establish a baseline exploration of the potential security threats from the metaverse, and in doing so, it highlighted several important issues that need to be addressed by Meta and the greater technological industry. In an ideal world, enhanced collaboration between a variety of industries will result in a safer, more robust metaverse for us all.

APPENDIX. SURVEY QUESTIONS AND RESPONSES

The following questions were asked of Meta's metaverse users.

- How frequently do you use Meta VR?
Daily, weekly, monthly, or yearly?
- How often do you interact socially in Meta VR?
Daily, weekly, monthly, or yearly?
Hours per day/week/month?
- How do you use Meta VR?
For work, for fun, for school, or for other purposes?
- Have you reported anyone's account in Meta VR for explicit behavior or content violations?
- Please describe any scenarios where you have been asked for money in Meta VR.
- Please describe any scenarios where you have been asked to contact someone offline about a financial opportunity in Meta VR.
- Please describe any scenarios where you have been approached about financial crime in Meta VR.
- Please describe any scenarios where you have been approached about an investment opportunity in Meta VR.
- Please describe any scenarios where you have been assaulted in Meta VR, including, but not limited to, the following: harassed (verbally), sexually harassment, violent speech, hateful speech, harassed (physically), groped, sexually assaulted, or simulated rape.

- Please describe any scenarios where you have encountered extremist content in Meta VR.
- Have you encountered children in social VR environments?
- Please describe any scenarios where you have encountered inappropriate content in Meta VR where children are users.
- Do you have children in your household using Meta VR?
- Do any children in your household have unsupervised access to Meta VR?
- Do you moderate the content the children in your household view in Meta VR?
- How has your use of Meta VR changed since you encountered the above situations?
- Please describe any scenarios where you have witnessed other people experiencing any of the incidents above.
- Do you think it is essential to address these situations in Meta VR? Why or why not?
- Can being the victim of a crime in Meta VR have long-lasting effects? Please elaborate as much or as little as you would like.

Please describe any scenarios where you have been approached about an investment opportunity in Meta VR.

I have been approached a few times about investment opportunities in Meta VRse. The first time was when a friend of mine mentioned that he had invested in the company and was seeing great returns. He suggested that I look into it as well. The second time was when I was contacted by a venture capitalist who was interested in investing in Meta VRse and wanted to discuss my potential involvement. Finally, I was contacted by a Meta VRse representative who was interested in getting me involved in the company's growth by offering me an opportunity to invest in the company.

Please describe any scenarios where you have been assaulted in Meta VR including, but not limited to the following: harassed (verbally), sexual harassment, violent speech, hateful speech, harassed (physically), groped, sexually assaulted, or simulated rape.

Harassed (verbally): I have been in Meta VR where I was walking around in a virtual world and a stranger shouted out inappropriate comments at me, using language that was derogatory and offensive.

Whether in Meta or in other online gaming scenarios, you may not be able to spend 15 seconds in a lobby waiting for a game to start without hearing extreme swearing, insults, or racist terms. It comes with the territory.

In MetaVR, I have been harassed verbally and subjected to hateful speech. I have also been groped, and sexually assaulted. On one occasion, I was simulating a scenario in which I was playing a victim of a simulated rape. I was verbally harassed by the perpetrator and I felt extremely uncomfortable and scared. I was also physically harassed with unwanted touches and was subjected to violent speech. This was a deeply traumatic experience for me and it made me feel very uncomfortable in MetaVR.

There was one time I was groped but it was very quick and the person left.

Please describe any scenarios where you have encountered extremist content in Meta VR.

Given that metaverse platforms allow users to look like whatever they want, its [sic] no surprise that some will choose avatars of controversial or extremist figures as a form of edgy humor. I've encountered users wearing avatars of Adolf Hitler, Joseph Stalin, and Osama Bin Laden on separate occasions. The users otherwise acted normal, but they were intentionally trying to disrupt or break into others' conversations to surprise/shock them

as a “prank.” These users seemed to be in their early-mid teens (anecdotally, based on their voices).

One scenario I encountered extremist content in Meta VR was when I was researching a particular topic in the metaverse. I found a group of users who were discussing and promoting extremist views and ideologies. This included content such as inflammatory rhetoric, calls to violence, and hateful language. I reported the group to the moderators and the content was quickly removed.

Have you encountered children in social VR environments?

Yes, often. The cheap cost of the Meta Quest 2, combined with the free-to-play social VR apps and difficulty in monitoring the child’s VR activity (It is not shown on an external screen, so the parent can’t “peek over their shoulder” to see what the child is doing) means many children end up in online spaces where they should not.

Yes, I have encountered children in social VR environments. Many virtual reality platforms, such as AltspaceVR, allow users to create avatars that are appropriate for all ages. As such, I have encountered children in these platforms, either through their own avatars or through their parents’ avatars.

Please describe any scenarios where you have encountered inappropriate content in Meta VR where children are users.

18+ virtual night club with alcohol in alt space, where a child entered and had to be asked to leave

As I said before, attending 18+ raves/parties is one of my favorite activities in VR. These events are adults in nature, with users drinking, dancing, and smoking (from their own homes, but together in VR) and since these events are public, sometimes minors find their way in through a discord, twitter invite, or whatever. I am a volunteer staff member for one such club in VRChat and have infrequently had underage users try to enter these events. They are removed from the world as soon as staff realizes they are underage, but sometimes they slip through the cracks because you can’t tell by the way they look. Nothing inappropriate happened to them when this has happened, but it’s generally just not a good environment for a minor to hang out in.

One scenario where I have encountered inappropriate content in Meta VR where children are users is when playing a game that has a chat feature. Some of the other players may use language or discuss topics that are not suitable for children. In addition, some games may feature violence or adult themes that are not suitable for children. In these cases, it is important to

monitor the content that children are exposed to and ensure that it is appropriate for their age.

Do you moderate the content the children in your household view in Meta VR?

Yes, I do moderate the content the children in my household view in Meta VR. I have set age-appropriate filters in place to ensure that they only see content that is suitable for their age level. I also actively monitor their usage and check in with them to make sure they are not accessing any inappropriate content.

How has your use of Meta VR changed since you encountered the above situations?

Since encountering these situations, my use of Meta VR has changed drastically. I now use it much more carefully and mindfully, making sure to double-check any configuration settings before beginning a project, making sure to keep backups of all my data, and being more mindful of the safety features and other features of the program. I also make sure to keep my work environment organized and well-maintained, so that I can easily access any needed files. Finally, I make sure to update the software regularly, so that I can take advantage of the latest features and fixes.

Since encountering the above situations, my use of Meta VR has changed in that I have become more mindful of the potential pitfalls of using this technology. I now take extra care to ensure that I am familiar with the features and capabilities of Meta VR before attempting to use it. I also try to remain aware of potential security risks, and take steps to ensure that my data and information is secure. Additionally, I am now more proactive in researching and staying up to date on the latest advancements in Meta VR technology.

Do you think it is essential to address these situations in Meta VR? Why or why not?

Yes, for the safety of children and others both online and offline.

I do think it is essential to address these situations in all VR platforms. The opportunities to contact unsuspecting and naive individuals will exponentially grow in the coming years as VR becomes more available and accessible by the general population.

Yes, because it is one more way someone with criminal intent can reach into your household.

Definitely. It is the next level of entertainment for households where the ramifications of VR interaction have not been tapped. Criminals will find ways to exploit weaknesses before they are announce through mainstream platforms as concerns.

Yes, if the platform will have underage children on it, it needs to be a safe environment.

Yes, I believe it is important in order for Meta to provide a safe environment for users. Since it's a social environment it should have norms and policies that have consequences for users who violate them. If not, the majority of the people who use their product will end up losing trust in the company.

Yes—besides being traumatic for a victim, I worry such situation in VR may lead to worse behaviors, including the same crimes, in the real world for some people.

Yes, it is essential to address these situations in Meta VR because they can potentially have a significant impact on the user experience. For example, if the virtual environment is not optimized for the user's hardware, it could result in poor performance or even crashes. Additionally, if the user interface is confusing or hard to use, it could lead to frustration and a bad user experience. Therefore, addressing these situations is essential to ensure the best possible experience for users.

Can being the victim of a crime in Meta VR have long-lasting effects? Please elaborate as much or as little as you would like.

Yes, it can cause lasting psychological effects for children to be groomed or otherwise exposed to sexually explicit behavior in virtual reality, or have such behavior be normalized in their virtual life, which is becoming harder for children to distinguish from reality.

Yeah. Anything that spills into the real world (financial crimes, fraud, etc.) and also people can experience real trauma through virtual environments. Just look at scary movies and how those can really traumatize people. Same concept.

While I have not experienced direct impacts from crime, I am certain the psychological affects [*sic*] of hate, violence, or sex crimes in a VR environment can be pervasive and detrimental to a person's wellbeing immediately and long after the incident. I believe it to be a parallel to physical versions of the same and possibly worse due to the likely stigma of the event occurring virtually. Any financial crime may be longer lasting than a cash version of the same since access to accounts may be inadvertently given.

Absolutely. It would change trust in that type of media.

I feel like it could. If someone engages in questionable behavior, acts, or discussions on VR and it is recorded, it could be used to exploit, blackmail, or discredit an individual.

Of course. Individual psychology is widely varied and an individual could consider themselves to be traumatized from a VR experience in the same ways a book or film could deeply affect someone.

I imagine so. You can always unplug, but can't ever forget events that you've seen and been apart [*sic*] of.

Yes, I believe so. VR/AR [augmented reality] is a fully immersive environment with visual stimuli replicating the real world. We see cases where cyber bullying and scams effect [*sic*] people with just online text messages, I imagine the effects are exacerbated in an AR/VR environment.

Yes, everyone takes things differently and people go through different things, so when a person does something wrong it might trigger the other person because of past trauma.

Crimes such as theft and assault in virtual worlds will affect real human beings and will be real crimes.

Yes—the effects can be similar to actual reality

Yes, being the victim of a crime in Meta VR can have long-lasting effects. Depending on the severity of the crime, victims can experience feelings of fear, anxiety, depression, and post-traumatic stress disorder (PTSD). These feelings can be exacerbated by the virtual nature of the crime, which can make the experience feel more intense and inescapable. Victims of Meta VR crime may also struggle with feelings of guilt or shame, or be reluctant to talk about the experience due to its virtual origin. Victims may also be reluctant to return to the virtual environment in which the crime occurred, or may struggle to trust other virtual users.

Yes, the mind is more easily tricked into believing that VR is real than most people would care to admit. Interactions in fully-embodied VR can be just as real as face-to-face interactions (In my opinion), and crime, harassment, and sexual assault in VR can have the same effect as experiencing it in person.

Yes, it is possible for being the victim of a crime in Meta VR to have long lasting effects. Depending on the type and severity of the crime, the victims may experience a range of emotions including fear, anxiety, depression, anger, and post-traumatic stress disorder. These feelings can last for months or even years after the crime has occurred. Victims may also experience physical and psychological effects such as difficulty sleeping, changes in

appetite, flashbacks, and avoidance of certain places or people. In addition, victims may have difficulty trusting people, developing relationships, and feeling safe in the virtual world. It is important for victims to seek help from a mental health professional if they are experiencing any of these effects, as they can be very difficult to cope with on their own.

I would assume it can. If you are very into the VR you will feel as if it is happening in real life to an extent. That could provoke very real feelings and trauma.

LIST OF REFERENCES

- American Academy of Child and Adolescent Psychiatry. "Internet Use in Children." October 2015. https://www.aacap.org/AACAP/Families_and_Youth/Facts_for_Families/FFF-Guide/Children-Online-059.aspx.
- American Library Association. "Hate Speech and Hate Crime." Accessed January 24, 2023. <https://www.ala.org/advocacy/intfreedom/hate>.
- Anderson, Janna, and Lee Rainie. *The Metaverse in 2040*. New York: Pew Research Center, 2022. <https://www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040/>.
- Anti-Defamation League. *Hate Is No Game: Harassment and Positive Social Experiences in Online Games 2021*. New York: Anti-Defamation League, 2021. <https://www.adl.org/resources/report/hate-no-game-harassment-and-positive-social-experiences-online-games-2021>.
- Armstrong, Kiah, and Ryan Bittan. "Metaverse Kidnapping: Missing Teen Found with Man She Met through Oculus Meta Program, Police Say." FOX8 WGHP, March 12, 2022. <https://myfox8.com/news/crime/metaverse-kidnapping-missing-teen-found-with-man-she-met-through-oculus-meta-program-police-say/>.
- Authentic8* (blog). "3 Roadblocks for Using OSINT in Law Enforcement." April 27, 2022. <https://authentic8.com/blog/3-roadblocks-using-osint-law-enforcement>.
- Baker-White, Emily. "Meta Wouldn't Tell Us How It Enforces Its Rules in VR, so We Ran a Test to Find Out." BuzzFeed News, February 11, 2022. <https://www.buzzfeednews.com/article/emilybakerwhite/meta-facebook-horizon-vr-content-rules-test>.
- Basu, Tanya. "The Metaverse Has a Groping Problem Already." *MIT Technology Review*, December 16, 2021. <https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/>.
- BBC News. "Second Life 'Child Abuse' Claim." May 9, 2007. <http://news.bbc.co.uk/2/hi/technology/6638331.stm>.
- Bell, Karissa. "How Meta Flunked Its First Year as a Metaverse Company." Engadget, December 20, 2022. <https://www.engadget.com/how-meta-flunked-its-first-year-as-a-metaverse-company-150049067.html>.
- bHaptics. "Home Page." Accessed January 26, 2023. <https://www.bhaptics.com/>.

- Bloomberg Professional Services* (blog). “Metaverse May Be \$800 Billion Market, Next Tech Platform.” December 1, 2021. <https://www.bloomberg.com/professional/blog/metaverse-may-be-800-billion-market-next-tech-platform/>.
- Bonifacic, Igor. “Investigation of VRChat Finds Rampant Child Grooming and Other Safety Issues.” *Engadget*, February 23, 2022. <https://www.engadget.com/bbc-vrchat-child-safety-report-193124305.html>.
- Boone, Jason. *Criminal Use of Social Media*. Fairmont, WV: National White Collar Crime Center, 2011. <https://vrnclearinghousefiles.blob.core.windows.net/documents/Criminal%20Use%20of%20Social%20Media.pdf>.
- Bowman, Cynthia. “How Much Do Twitch Streamers Make? 2023 Top Earners.” *GO Banking Rates*, April 27, 2023. <https://www.gobankingrates.com/money/entrepreneur/how-much-do-twitch-streamers-make/>.
- Brown, Emily, and Paul Cairns. “A Grounded Investigation of Game Immersion.” In *CHI '04 Extended Abstracts on Human Factors in Computing Systems*, 1297–1300. New York: Association for Computing Machinery, 2004. <https://doi.org/10.1145/985921.986048>.
- Carlton, Bobby. “Feel Rain Fall in VR with Full-Body Teslasuit.” *VR Scout*, July 12, 2021. <https://vrscout.com/news/feel-rain-fall-in-vr-with-full-body-teslasuit/>.
- Caserman, Polona, Miriam Cornel, Michelle Dieter, and Stefan Göbel. “A Concept of a Training Environment for Police Using VR Game Technology.” In *Proceedings of the 2018 Joint International Conference on Serious Games*, edited by Stefan Göbel, Augusto Garcia-Agundez, Thomas Tregel, Minhua Ma, Jannicke Baalsrud Hauge, Manuel Oliveira, Tim Marsh, and Polona Caserman, 11243:175–81. Lecture Notes in Computer Science. Cham, Switzerland: Springer International Publishing, 2018. https://doi.org/10.1007/978-3-030-02762-9_18.
- Cela, Anna. “Is the Structure of Metaverse Centralized or Decentralized?” *TechStar* (blog), December 7, 2022. <https://www.techstar.it/en/blog/is-the-structure-of-metaverse-centralized-or-decentralized/>.
- Cheong, Ben Chester. “Avatars in the Metaverse: Potential Legal Issues and Remedies.” *International Cybersecurity Law Review* 3, no. 2 (2022): 467–94. <https://doi.org/10.1365/s43439-022-00056-9>.
- Children’s Society. “Virtual Reality and Child Safety.” March 3, 2023. <https://www.childrenssociety.org.uk/what-we-do/blogs/virtual-reality-and-child-safety>.
- Choi, Sam Jungyun, Dan Cooper, Bart Szewczyk, and Sebastian Vos. “Regulating the Metaverse in Europe.” *Covington Global Policy Watch*, April 11, 2023. <https://www.globalpolicywatch.com/2023/04/regulating-the-metaverse-in-europe/>.

- Choo, Kim-Kwang Raymond, and Russell G. Smith. "Criminal Exploitation of Online Systems by Organised Crime Groups." *Asian Journal of Criminology* 3, no. 1 (June 2008): 37–59. <https://doi.org/10.1007/s11417-007-9035-y>.
- Cloudflare. "What Is Swatting? How to Prevent Swatting." Accessed January 26, 2023. <https://www.cloudflare.com/learning/security/glossary/what-is-swatting/>.
- Cole, James. "Radicalisation in Virtual Worlds: Second Life through the Eyes of an Avatar." *Journal of Policing, Intelligence and Counter Terrorism* 7, no. 1 (April 2012): 66–79. <https://doi.org/10.1080/18335330.2012.653197>.
- Coleman, Sabryne. "You Only Live Twice: How the First Amendment Impacts Child Pornography in Second Life." *Loyola of Los Angeles Entertainment Law Review* 29, no. 2 (2009): 193–232. <https://digitalcommons.lmu.edu/elr/vol29/iss2/2>.
- Common Sense Media. "Common Sense Privacy Standard Privacy Report for Oculus." December 6, 2022. <https://privacy.commonsense.org/privacy-report/Oculus>.
- Council of the European Union. "Online Gaming in the Context of the Fight against Terrorism." Official memorandum. Brussels: Council of the European Union, 2020. <https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf>.
- Crawford, Angus, and Tony Smith. "Metaverse App Allows Kids into Virtual Strip Clubs." BBC News, February 23, 2022. <https://www.bbc.com/news/technology-60415317>.
- Crunchbase. "Oculus Acquired by Meta." Accessed March 6, 2023. <https://www.crunchbase.com/acquisition/facebook-acquires-oculus-vr--30357598>.
- Dang, Brandon, Martin J. Riedl, and Matthew Lease. "But Who Protects the Moderators? The Case of Crowdsourced Image Moderation." arXiv, 2020. <https://doi.org/10.48550/arXiv.1804.10999>.
- De Koster, Willem, and Dick Houtman. "'Stormfront Is Like a Second Home to Me': On Virtual Community Formation by Right-Wing Extremists." *Information, Communication & Society* 11, no. 8 (2008): 1155–76. <https://doi.org/10.1080/13691180802266665>.
- Di Pietro, Roberto, and Stefano Cresci. "Metaverse: Security and Privacy Issues." In *Proceedings of the Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications*, 281–88. Piscataway, NJ: IEEE, 2021. <https://doi.org/10.1109/TPSISA52974.2021.00032>.
- Elson, Joel, Austin C. Doctor, and Sam Hunter. "Metaverse, Social Media, Terrorism." Homeland Security Newswire, January 10, 2022. <https://www.homelandsecuritynewswire.com/dr20220110-the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too>.

- European Commission. "A Europe Fit for the Digital Age." Accessed April 17, 2023. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en#.
- European Union Agency for Law Enforcement Cooperation. *Policing in the Metaverse: What Law Enforcement Needs to Know*. Luxembourg: Publications Office of the European Union, 2022. <https://data.europa.eu/doi/10.2813/81062>.
- Farivar, Cyrus. "Extremists Creep into Roblox, an Online Game Popular with Children." NBC News, August 21, 2019. <https://www.nbcnews.com/tech/tech-news/extremists-creep-roblox-online-game-popular-children-n1045056>.
- Federal Bureau of Investigation, Springfield Field Office. "Internet Crime Complaint Center Releases 2022 Statistics." March 22, 2023. <https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics>.
- Ferguson, Katelyn, Moon Jung Kim, and Martyna Dobrowolska. "The Role of Video Games and Online Platforms in Terrorist Radicalization and Recruitment." Counterterrorism Group, June 17, 2021. <https://www.counterterrorismgroup.com/post/the-role-of-video-games-and-online-platforms-in-terrorist-radicalization-and-recruitment>.
- Garcia-Ruiz, Miguel A., Miguel Vargas Martin, Amin Ibrahim, Arthur Edwards, and Raul Aquino-Santos. "Combating Child Exploitation in Second Life." In *Proceedings of the 2009 IEEE Toronto International Conference on Science and Technology for Humanity*, 761–66. Piscataway, NJ: IEEE, 2009. <https://doi.org/10.1109/TIC-STH.2009.5444398>.
- Girvan, Carina. "What Is a Virtual World? Definition and Classification." *Educational Technology Research and Development* 66, no. 5 (October 2018): 1087–1100. <https://doi.org/10.1007/s11423-018-9577-y>.
- Gottschalk, Simon. "The Presentation of Avatars in Second Life: Self and Interaction in Social Virtual Spaces." *Symbolic Interaction* 33, no. 4 (2010): 501–25. <https://doi.org/10.1525/si.2010.33.4.501>.
- Government Accountability Office. "To Address Emerging Privacy Issues, Congress Should Consider Comprehensive Legislation." September 13, 2022. <https://www.gao.gov/blog/address-emerging-privacy-issues-congress-should-consider-comprehensive-legislation>.
- Gourlay, Chris, and Abul Taher. "Virtual Jihad Hits Second Life website." *Times* (United Kingdom), August 5, 2007. <https://www.thetimes.co.uk/article/virtual-jihad-hits-second-life-website-l2cf6vm92pb>.

- Guadagno, Rosanna E., Adam Lankford, Nicole L. Muscanell, Bradley M. Okdie, and Debra M. McCallum. "Social Influence in the Online Recruitment of Terrorists and Terrorist Sympathizers: Implications for Social Psychology Research." *Revue internationale de psychologie sociale* [International journal of social psychology] 23, no. 1 (2010): 25–56. <https://www.cairn.info/revue-internationale-de-psychologie-sociale-2010-1-page-25.htm>.
- Hadad, Avi. "Just like IRL, the Metaverse Requires Infrastructure. We Don't Have It Yet." TechCrunch, April 4, 2022. <https://techcrunch.com/2022/04/04/just-like-irl-the-metaverse-requires-infrastructure-we-dont-have-it-yet/>.
- Hamilton, Ian. "Facebook: Beat Saber 'Saved' Oculus Quests." Upload VR, March 29, 2021. <https://uploadvr.com/facebook-beat-saber-imu/>.
- Harris, Jamie. "Meta Police: Inside Interpol's Secret Virtual HQ as Cops Plan to Hunt Criminals in the Metaverse." *U.S. Sun*, February 6, 2023. <https://www.the-sun.com/tech/7319286/interpol-metaverse-crime-police/>.
- Hood, Callum. "New Research Shows Metaverse Is Not Safe for Kids." Center for Countering Digital Hate, December 19, 2021. <https://counterhate.com/blog/new-research-shows-metaverse-is-not-safe-for-kids/>.
- Howcroft, Elizabeth. "Crypto Crime Hits Record \$20 Bln in 2022, Report Says." Reuters, January 12, 2023. <https://www.reuters.com/business/finance/crypto-crime-hits-record-20-bln-2022-report-says-2023-01-12/>.
- Investopedia. "What Is the Linden Dollar?" Accessed January 26, 2023. <https://www.investopedia.com/terms/l/linden-dollar.asp>.
- Irwin, Angela S. M., and Jill Slay. "Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft." In *Proceedings of the First International Cyber Resilience Conference*, 41–50. Perth: Edith Cowan University, 2010.
- Irwin, Angela S. M., Jill Slay, Kim-Kwang Raymond Choo, and Lin Lui. "Money Laundering and Terrorism Financing in Virtual Environments: A Feasibility Study." *Journal of Money Laundering Control* 17, no. 1 (2014): 50–75. <https://doi.org/10.1108/JMLC-06-2013-0019>.
- Jeter, Sinclair, and Darris Taylor. "Terrorist Presence in Virtual Worlds: Using Second Life as a Case Study." *International Journal of Interdisciplinary Social Sciences: Annual Review* 6, no. 10 (2012): 1–6. <https://cgscholar.com/bookstore/works/terrorist-presence-in-virtual-worlds>.
- Johnson, Dave. "The Oculus Quest Is Sold Out Pretty Much Everywhere Right Now." CNET, September 9, 2020. <https://www.cnet.com/deals/where-you-can-buy-hard-to-find-oculus-quest-right-now/>.

- Kahila, Juho, Jaana Viljaranta, Sanni Kahila, Satu Piispa-Hakala, and Henriikka Vartiainen. "Gamer Rage—Children's Perspective on Issues Impacting Losing One's Temper While Playing Digital Games." *International Journal of Child-Computer Interaction* 33 (September 2022): 100513. <https://doi.org/10.1016/j.ijcci.2022.100513>.
- Kalis, Brian, Jenica McHugh, Kaveh Safavi, and Andrew Truscott. *Meet Me in the Metaverse: Accenture Digital Health Technology Vision 2022*. Accenture, 2022. <https://www.accenture.com/us-en/insights/health/digital-health-technology-vision>.
- Kalning, Kristin. "If Second Life Isn't a Game, What Is It?" NBC News, March 11, 2007. <https://www.nbcnews.com/id/wbna17538999>.
- Kan, Michael. "Police in the Metaverse? Interpol Urges Law Enforcement to Embrace VR Tech." *PC Magazine*, October 21, 2022. <https://www.pcmag.com/news/police-in-the-metaverse-interpol-urges-law-enforcement-to-embrace-vr-tech>.
- Kang, Cecilia. "As Europe Approves New Tech Laws, the U.S. Falls Further Behind." *New York Times*, April 22, 2022. <https://www.nytimes.com/2022/04/22/technology/tech-regulation-europe-us.html>.
- KAT VR. "KAT Walk C2 Core." Accessed April 18, 2023. <https://www.kat-vr.com/products/kat-walk-c2>.
- Kelly, Girard, Jeff Graham, Jill Bronfman, and Steve Garton. *Privacy of Virtual Reality: Our Future in the Metaverse and Beyond*. San Francisco: Common Sense Media, 2022. <https://www.common sense media.org/sites/default/files/research/report/privacy-of-virtual-reality-our-future-in-the-metaverse-and-beyond.pdf>.
- Kish, Stephen. "Massive Multiplayer Games a Platform for Terrorism?" Patrick Henry College, May 17, 2017. <https://www.phc.edu/intelligencer/massive-multiplayer-games-a-platform-for-terrorism>.
- Kostov, Georgi Yordanov. "Fostering Player Collaboration within a Multimodal Co-located Game." Master's thesis, University of Applied Sciences Upper Austria, Hagenberg, 2015. https://www.researchgate.net/figure/The-Sword-of-Damocles-by-Ivan-Sutherland_fig2_291516650.
- Kumar, Nitin. "Six Unaddressed Legal Concerns for the Metaverse." *Forbes*, February 17, 2022. <https://www.forbes.com/sites/forbestechcouncil/2022/02/17/six-unaddressed-legal-concerns-for-the-metaverse/>.
- Lapin, Nicole. "Explaining Crypto's Volatility." *Forbes*, December 23, 2021. <https://www.forbes.com/sites/nicolelapin/2021/12/23/explaining-cryptos-volatility/>.

- Laub, Zachary. "Hate Speech on Social Media: Global Comparisons." Council on Foreign Relations, June 7, 2019. <https://www.cfr.org/backgrounder/hate-speech-social-media-global-comparisons>.
- Lenhart, Amanda, Aaron Smith, Monica Anderson, Maeve Duggan, and Andrew Perrin. "Chapter 3: Video Games Are Key Elements in Friendships for Many Boys." In *Teens, Technology & Friendships: Video Games, Social Media and Mobile Phones Play an Integral Role in How Teens Meet and Interact with Friends*, 41–52. Washington, DC: Pew Research Center, 2015. <https://www.pewresearch.org/internet/2015/08/06/chapter-3-video-games-are-key-elements-in-friendships-for-many-boys/>.
- Leyden, Ian. "How to Tame the New Wild-Wild West: Potential Lassos for Virtual Crime." South Orange, NJ: Seton Hall University, 2010. https://scholarship.shu.edu/student_scholarship/63.
- Liu, Xinxiong, Jing Zhang, Guoxiang Hou, and Zenan Wang. "Virtual Reality and Its Application in Military." *IOP Conference Series: Earth and Environmental Science* 170, no. 3 (2018): 1–7. <https://doi.org/10.1088/1755-1315/170/3/032155>.
- Lufkin, Bryan. "How Online Gaming Has Become a Social Lifeline." BBC, December 16, 2020. <https://www.bbc.com/worklife/article/20201215-how-online-gaming-has-become-a-social-lifeline>.
- Mak, Aaron. "I Was a Bouncer in the Metaverse." *Slate*, May 9, 2022. <https://slate.com/technology/2022/05/metaverse-content-moderation-virtual-reality-bouncers.html>.
- McKinsey & Company. "Let's Meet in the Metaverse." August 4, 2022. <https://www.mckinsey.com/featured-insights/sustainable-inclusive-growth/chart-of-the-day/lets-meet-in-the-metaverse>.
- Meek-Prieto, Caroline. "Just Age Playing Around—How Second Life Aids and Abets Child Pornography." *North Carolina Journal of Law & Technology* 9, no. 6 (2008): 88–113. <http://scholarship.law.unc.edu/ncjolt/vol9/iss3/6>.
- Meta. "About the Metaverse." Accessed January 26, 2023. <https://about.meta.com/metaverse/>.
- . "Meta for Work: Four Predictions for the Future of Work." Accessed December 1, 2022. <https://www.meta.com/work/predictions/>.
- . "This Is Meta Quest Pro." Accessed April 18, 2023. <https://www.meta.com/quest/quest-pro/>.
- . "What Is the Metaverse?" Accessed January 26, 2023. <https://about.meta.com/what-is-the-metaverse/>.

- Meta Quest Apps & Games. "VRChat: Reviews." Accessed August 10, 2023. <https://www.oculus.com/experiences/quest/1856672347794301/>.
- Miller, Haylie L., and Nicoleta L. Bugnariu. "Level of Immersion in Virtual Environments Impacts the Ability to Assess and Teach Social Skills in Autism Spectrum Disorder." *Cyberpsychology, Behavior and Social Networking* 19, no. 4 (2016): 246–56. <https://doi.org/10.1089/cyber.2014.0682>.
- Montelli, Chrissy. "What Does 'NPC' Mean? Understanding Non-player Characters, an Important Aspect of Any Video Game." *Insider*, May 28, 2021. <https://www.businessinsider.com/guides/tech/npc-meaning>.
- Moy, Christine, and Adit Gadgil. *Opportunities in the Metaverse: How Businesses Can Explore the Metaverse and Navigate the Hype vs. Reality*. New York: JPMorgan Onyx, 2022. <https://www.jpmorgan.com/content/dam/jpm/treasury-services/documents/opportunities-in-the-metaverse.pdf>.
- Moyer, Melinda Wenner. "Kids as Young as 8 Are Using Social Media More than Ever, Study Finds." *New York Times*, March 24, 2022. <https://www.nytimes.com/2022/03/24/well/family/child-social-media-use.html>.
- National Center for Missing and Exploited Children. "CyberTipline 2022 Report." Accessed April 18, 2023. <http://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.html>.
- National Center on Sexual Exploitation. "The Dirty Dozen List: Meta." Accessed January 24, 2023. <https://endsexualexploitation.org/meta/>.
- Nationwide SAR Initiative. "Suspicious Activity Reporting Indicators and Behaviors." February 2016. https://www.dhs.gov/sites/default/files/publications/16_0208_NSI_SAR-Indicators-Behaviors-Tools-Analysts-Investigators.pdf.
- New World Notes* (blog). "Second Life Usage Now Higher than Its 2007 Hype Level Period?" June 22, 2020. <https://nwn.blogs.com/nwn/2020/06/second-life-sl-linden-lab-mau-concurrency.html>.
- Nielsen. "3, 2, 1 Go! Video Gaming Is at an All-Time High during COVID-19." June 2020. <https://www.nielsen.com/insights/2020/3-2-1-go-video-gaming-is-at-an-all-time-high-during-covid-19/>.
- Nightfreeze* (blog). "The Great Scam." Accessed June 21, 2022. <http://www.wirm.net/nightfreeze/part1.html>.
- Ninja. "Jujutsu Kaisen Collab Is in Fortnite All Day Games around 10am Central w/Timthetatman and Cloakzy." Twitch. Accessed January 24, 2023. <https://www.twitch.tv/ninja>.

- O'Brien, Natalie. "Virtual Terrorists." *Australian*, July 31, 2007. Lexis-Nexis.
- Oentoro, Andre. "5 VR Accessories You Need for the Next-Level Immersion." AR Post, July 27, 2022. <https://arpost.co/2022/07/27/5-vr-accessories-next-level-immersion/>.
- Olen VR. "VR Gun Stocks." Accessed March 3, 2023. <https://www.olenvr.com/vr-gun-stocks>.
- Oliva, David, Brita Somerkoski, K. Tarkkanen, Anttoni Lehto, and Mika Luimula. "Virtual Reality as a Communication Tool for Fire Safety—Experiences from the VirPa Project." In *Proceedings of the GamiFIN Conference 2019*, 241–52. CEUR Workshop Proceedings, 2019. <http://ceur-ws.org/Vol-2359/paper21.pdf>.
- Omnifinity. "Home Page." Accessed January 26, 2023. <https://www.omnifinity.se/>.
- . "Omnideck 6 at I/ITSEC 2014." Video, 1:19. YouTube, December 1, 2014. <https://www.youtube.com/watch?v=wPffziOrE6Y>.
- Oremus, Will. "Kids Are Flocking to Facebook's 'Metaverse.' Experts Worry Predators Will Follow." *Washington Post*, February 7, 2022. <https://www.washingtonpost.com/technology/2022/02/07/facebook-metaverse-horizon-worlds-kids-safety/>.
- O'Rourke, Simon. "Virtual Radicalisation: Challenges for Police." In *Proceedings of the Eighth Australian Information Warfare and Security Conference*, 29–35. Perth: Edith Cowan University, 2007. <https://doi.org/10.4225/75/57A83C57BEFAB>.
- Pallavicini, Federica, Luca Argenton, Nicola Toniazzi, Luciana Aceti, and Fabrizia Mantovani. "Virtual Reality Applications for Stress Management Training in the Military." *Aerospace Medicine and Human Performance* 87, no. 12 (2016): 1021–30. <https://doi.org/10.3357/AMHP.4596.2016>.
- Perez, Sarah. "Twitch Breaks Records Again in Q2, Topping 5B Total Hours Watched." TechCrunch, July 1, 2020. <https://techcrunch.com/2020/07/01/twitch-breaks-records-again-in-q2-topping-5b-total-hours-watched/>.
- PlayTracker. "VRChat Stats." Accessed February 27, 2023. <https://playtracker.net/insight/game/2704>.
- Ravenscraft, Eric. "What Is the Metaverse, Exactly?" *Wired*, November 25, 2021. <https://www.wired.com/story/what-is-the-metaverse/>.
- Ray, Shawn. "The Metaverse Is Coming—Who Will Police It?" Police1, January 30, 2023. <https://www.police1.com/investigations/articles/the-metaverse-is-coming-who-will-police-it-ttPcF7hT9wrhfvha/>.

- r/gaming. “Wiki.” Reddit. Accessed January 27, 2023. <https://www.reddit.com/r/gaming/wiki/index/>.
- Robertson, Derek. “Crimefighting in the Metaverse.” Politico, April 13, 2022. <https://politi.co/3EanPxP>.
- Roblox Support. “Experience Guidelines and Age Recommendations.” Accessed January 19, 2023. <https://en.help.roblox.com/hc/en-us/articles/8862768451604-Age-Recommendations>.
- Roebuck, Jeremy. “Philly Feds Help Dismantle Popular Crypto Money-Laundering Site Responsible for Cleaning \$3 Billion in Illicit Funds.” *Philadelphia Inquirer*, March 15, 2023. <https://www.inquirer.com/news/chip-mixer-crypto-bitcoin-seized-ming-quoc-nguyen-charges-20230315.html>.
- Ruskin, Matthew S. “Playing in the Dark How Online Games Provide Shelter for Criminal Organizations in the Surveillance Age.” *Arizona Journal of International & Comparative Law* 31, no. 3 (2014): 875–908. <http://arizona-journal.org/wp-content/uploads/2015/09/10-Ruskin.pdf>.
- Schroeder, Ralph. “Defining Virtual Worlds and Virtual Environments.” *Journal for Virtual Worlds Research* 1, no. 1 (July 2008): 1–3. <https://jvwr-ojs-utexas.tdl.org/jvwr/article/view/294/248>.
- Second Life. “Home Page.” Accessed January 26, 2023. <https://secondlife.com/>.
- Shutler, Ali. “Some Metaverse Apps Are ‘Dangerous by Design’ Claims Children’s Charity.” NME, February 23, 2022. <https://www.nme.com/news/gaming-news/some-metaverse-apps-are-dangerous-by-design-claims-childrens-charity-3168044>.
- SideQuest. “Decentraland VR.” Accessed April 17, 2023. <https://sidequestvr.com/app/11626/decentraland-vr>.
- Slater, Mel, and Sylvia Wilbur. “A Framework for Immersive Virtual Environments (FIVE): Speculations on the Role of Presence in Virtual Environments.” *Presence: Teleoperators and Virtual Environments* 6, no. 6 (1997): 603–16. <https://doi.org/10.1162/pres.1997.6.6.603>.
- Smith, Davy. “Multiple Identities, Security, and the Growth of the Metaverse.” MaddyNess, December 5, 2022. <https://www.maddyNess.com/uk/2022/12/05/multiple-identities-security-and-the-growth-of-the-metaverse/>.
- Song, Victoria. “Meta Quest Users Can Now Track Their Heart Rate in VR Workouts.” Verge, January 11, 2023. <https://www.theverge.com/2023/1/11/23550611/meta-quest-heart-rate-health-connect-android>.

- Squire, Kurt. "Open-Ended Video Games: A Model for Developing Learning for the Interactive Age." In *The Ecology of Games: Connecting Youth, Games, and Learning*, edited by Katie Salen, 167–98. Cambridge, MA: MIT Press, 2008. <https://doi.org/10.1162/dmal.9780262693646.167>.
- Stanton, Rich. "If Roblox's Daily Users Were a Country, It Would Be Bigger than Canada." PC Gamer, February 16, 2022. <https://www.pcgamer.com/if-robloxs-daily-users-were-a-country-it-would-be-bigger-than-canada/>.
- Steam. "Elite Dangerous." Accessed March 3, 2023. https://store.steampowered.com/app/359320/Elite_Dangerous/.
- Steiger, Miriah, Timir J. Bharucha, Sukrit Venkatagiri, Martin J. Riedl, and Matthew Lease. "The Psychological Well-Being of Content Moderators: The Emotional Labor of Commercial Moderation and Avenues for Improving Support." In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–14. New York: Association for Computing Machinery, 2021. <https://doi.org/10.1145/3411764.3445092>.
- Stein, Scott. "After a Turbulent 2022, What Happens to Meta's Metaverse in 2023?" CNET, December 20, 2022. <https://www.cnet.com/tech/computing/after-a-turbulent-2022-what-happens-to-metas-metaverse-in-2023/>.
- Steuer, Jonathan. "Defining Virtual Reality: Dimensions Determining Telepresence." In *Communication in the Age of Virtual Reality*, edited by Frank Biocca and Mark R. Levy, 33–56. Hillsdale, NJ: Lawrence Erlbaum Associates, 1995.
- Stokes, Robert. "Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar." *Information & Communications Technology Law* 21, no. 3 (2012): 221–36. <https://doi.org/10.1080/13600834.2012.744225>.
- Tassi, Paul. "'Fortnite' Legend Ninja Talks Twitch Fame and Fortune, and the Game That Got Him There." *Forbes*, March 13, 2018. <https://www.forbes.com/sites/insertcoin/2018/03/13/fortnite-legend-ninja-talks-twitch-fame-and-fortune-and-the-game-that-got-him-there/>.
- Tech Policy Press. "Transcript: Innovation, Data, and Commerce Subcommittee Hearing on Data Privacy." March 2, 2023. <https://techpolicy.press/transcript-innovation-data-and-commerce-subcommittee-hearing-on-data-privacy/>.
- Teslasuit. "Home Page." Accessed April 18, 2023. <https://teslasuit.io/>.
- Troughton, James. "Roblox Is Cracking Down on Players Recreating School Shootings in-Game." *Gamer*, August 19, 2021. <https://www.thegamer.com/roblox-school-shootings/>.

- Ugelow, Lisa, and Lance Hoffman. "Fighting on a New Battlefield Armed with Old Laws: How to Monitor Terrorism in the Virtual World." *University of Pennsylvania Journal of Constitutional Law* 14, no. 4 (2012): 1035–76. <https://scholarship.law.upenn.edu/jcl/vol14/iss4/5>.
- United Nations Counter-Terrorism Centre. "Examining the Intersection between Gaming and Violent Extremism: Executive Summary." Accessed January 26, 2023. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/221005_execute_summary_on_gaming_ve.pdf.
- Villar, Toin. "What Is Second Life? A Brief History of the Metaverse." Make Use Of, April 11, 2022. <https://www.makeuseof.com/what-is-second-life-history-metaverse/>.
- Virtual Reality Society. "History of Virtual Reality." Accessed September 21, 2022. <https://www.vrs.org.uk/virtual-reality/history.html>.
- . "Virtual Reality Immersion." Accessed January 26, 2023. <https://www.vrs.org.uk/virtual-reality/immersion.html>.
- Wild. "What VR Headsets Are Supported in the Wild?" August 2, 2022. <https://thewild.com/help/vr-headset-support>.
- Wired. "Second Life: Facts for the Visitor." October 1, 2006. <https://www.wired.com/2006/10/slfacts/>.
- Witmer, Bob G., and Michael J. Singer. "Measuring Presence in Virtual Environments: A Presence Questionnaire." *Presence: Teleoperators and Virtual Environments* 7, no. 3 (1998): 225–40. <https://doi.org/10.1162/105474698565686>.
- World Wide Web Foundation. "Online Abuse in the Metaverse Untangled." February 23, 2022. <https://webfoundation.org/2022/02/online-abuse-in-the-metaverse-untangled/>.
- Wu, Katherine J. "Radical Ideas Spread through Social Media. Are the Algorithms to Blame?" NOVA Next, March 28, 2019. <https://www.pbs.org/wgbh/nova/article/radical-ideas-social-media-algorithms/>.
- Yin, Elizabeth, Mary Moynihan, and Alexandra Walsh. "Regulating the Metaverse." *Regulatory Review*, January 7, 2023. <https://www.theregreview.org/2023/01/07/saturday-seminar-regulating-the-metaverse/>.
- Zhu, Ling. *The Metaverse: Concepts and Issues for Congress*. CRS Report No. R47224. Washington, DC: Congressional Research Service, 2022. <https://crsreports.congress.gov/product/pdf/R/R47224>.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California



DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

WWW.NPS.EDU

WHERE SCIENCE MEETS THE ART OF WARFARE