RESPONSIBLE METAVERSE ALLIANCE

POLICING IN THE METAVERSE

Challenges and Opportunities for Disruption

Discussion Paper

Second in the 'Policing in the Metaverse' Series

November 2023

ACKNOWLEDGEMENTS

The Responsible Metaverse Alliance (RMA) acknowledges the traditional owners of the land we work from in Australia, and pay our respect to elders past and present. We thank Aboriginal and Torres Strait Islander people for their continued knowledge, wisdom and connection to the unceded lands and waters upon which we raise our families and share in community. Always was, and always will be, Aboriginal Land.

The RMA is an organisation built on collaboration with partners from many sectors and nations. In particular, we want to acknowledge those who have committed their time, expertise and wisdom to this body of work. In particular, the individuals who contributed and/or presented their work which sparked such valuable discussion at this Think Tank:

Speakers: **Dr Catriona Wallace,** Founder, Responsible Metaverse Alliance
Prof. Alana Maurushat, Cybersecurity and Behaviour at Western Sydney University
Peter Price AM, Director, Crime Stoppers Australia

We also acknowledge the many other individuals and organisations who have participated in and contributed to this Think Tank and our broader body of work. See the Discussion Paper from the first Think Tank in this session here.

CONTENTS

KEY TERMS & DEFINITIONS

Metaverse	**"Persistent and immersive simulated worlds that are experienced in the first person by groups of simultaneous users who share a strong sense of mutual presence"** description by Dr Louis Rosenberg, Chief Scientist at the Responsible Metaverse Alliance. Throughout this paper, we use the term 'Metaverse' to refer to 'immersive technologies'.
A.I.	**Artificial Intelligence.** The use of A.I. in the Metaverse is quickly becoming ubiquitous and requires a focused report to cover all of the dimensions involved.
Cybercrime	**Criminal activities carried out through the use of computers or online.** Can include financial crime, crimes against children, assault and sexual violence, terrorism related crime, acts intended to induce fear or emotional distress, crimes against public safety, coercion, property crime, intellectual property crime, among others.
Immersive Technologies	**Typically refers to multi-sensory technologies.** A collective term used to include Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR), Volumetric Video Capture, 360 Degree Video, Haptics.

INTRODUCTION

The Metaverse and immersive technologies provide a plethora of opportunities to improve the lives of a vast number of people and communities. As with all technological advancements, these opportunities also bring dynamic challenges for keeping users safe from online criminal behaviour, and while this responsibility is shared across governments, regulators, companies and the community, the lionshare falls upon the shoulders of law enforcement agencies. The new law enforcement challenges that emerged through the adoption of digital and online technologies over the last few decades saw mostly responsive legislation, regulation and enforcement implemented, meaning that cybercrime has typically been addressed after the harm was inflicted. This can largely be avoided in this new era of immersive technologies, as there are significant opportunities for learnings to bring forward and build upon - alongside the increasing recognition of safety-by-design principles.

Cybercrime is a continually evolving area of practice, but it is broadly recognised that relying on prosecution has always been limited in impact, and that most law enforcement and mitigation of crimes online is achieved through prevention and disruption strategies. Given this, along with the lack of effective regulation that holds platforms accountable, or empowers law enforcement to prevent and restrict criminals online, the Response Metaverse Alliance held our second 'Policing in the Metaverse' Think Tank in October 2023 with a focus on disruption strategies and to outline the needs and approach required for law enforcement.

Through the discussion, participants revisited specific online crimes and challenges that were explored in the first Think Tank, including the challenge of cross-jurisdictional enforcement; digital literacy of law enforcement; inadequacy of reactive responses to protect the public in the long term; the gaps in regulation (including the unmet low bar that has been set on basic consumer safety standards); a deeper dive on the role of AI; as well as the challenges of increased anonymity and the use of avatars. This conversation served as the backdrop for an exploration of the specific learnings available from the field of cybercrime, progressing into an exploration of an approach for policing the Metaverse into the future.

> *"If we talk to what the responses could look like from a law enforcement perspective, they tend to be potential reactive responses, and they are never going to be satisfactory for protecting the public long term"*
>
> *- Participant quote*

AREAS OF EXPLORATION

Through this Think Tank, participants discussed a number of topics related to disruption strategies in the Metaverse, the available learnings from the field of cybersecurity, as well as the new dimensions of the Metaverse that require deeper consideration as law enforcement agencies strengthen their approach and coordination.

Learnings From Cybersecurity

The perspective on cybercrime of most people is distorted due to the nature of the reporting on crimes committed, and the lack of awareness of how many are prevented. Major data breaches are always a newsworthy event, but security teams at major companies or law enforcement will rarely speak about those they prevent - and for good reason. The fact that cybercrime prevention is more common than not, means that experts in the field have significant experiences and successes to build on and bring into the crime prevention in the Metaverse.

There is a perception among law enforcement - and echoed by participants in our Think Tank - that the Metaverse has not generated entirely new groups of criminals, rather that we see the same criminal groups evolving their activities to leverage the new opportunities the Metaverse presents them. This has several implications, firstly that the approach of law enforcement should be focused on known perpetrators and groups, with resources committed to better understanding the new dimensions of existing cybercrimes in the Metaverse. Many of these crimes have been discussed in the first Think Tank in this series, and include challenges already known to law enforcement that are evolving in the Metaverse. The use of cryptocurrency is a notable example here, which has proven to be a significant challenge for tracking crimes, and will continue to do so in the Metaverse, opening new ways for theft and the movement of funds.

> *"It's not like there's suddenly a million new cybercriminals all marching in tune to exploit the Metaverse. It comes from deep organised criminal syndicates who have been in the space for a long time, who are innovative, and they move and adopt new technologies and new methods to do the same things they've always done, only it's in a different platform"*
>
> - Participant quote

There are of course new dynamics of the Metaverse that are important for law enforcement to consider, and to prepare and develop strategies to mitigate. These unknown dynamics discussed are worthy of further and deeper consideration in the preparedness and strategies of law enforcement agencies. They include an acknowledgement of a gap in understanding around how real world events will play out in the Metaverse. As much as we have now built a collective understanding and expectation of the impacts of elections and electoral disinformation online, or the hate speech generated following horrific events such as those currently unfolding in Palestine, we do lack a nuanced understanding of how the Metaverse will change these threats to users and social cohesion. Further, there is a lack of analysis around how well

equipped the existing architecture of law enforcement is to manage emergent threats. It was clear that law enforcement would benefit from concerted initiatives to better understand what the risks are, and how to respond or address them.

In understanding the parallels, learnings and gaps identified from the field of cybercrime prevention, we saw a robust discussion around how despite the changes to crimes and criminal behaviour, the basic principles of law enforcement and human rights do not fundamentally change with the adoption of new technologies. Amongst this conversation, there was also a recognition that some safety-by-design principles adopted for the Metaverse can undermine personal and data security. And so there is a real need for balancing effective policing with human rights, which requires an adaptation of approaches and tactics, more so than fundamental changes to law enforcement at this stage.

> *"As much as the technology is raising new questions and issues, and is confronting us with things moving at such speed - the basic principles of human rights and of law enforcement are still exactly the same. And just need to be applied in this new way into a new technology"*
>
> *- Participant quote*

Got To Be In It, To Police It

A theme that has been prominent through all of our work on ensuring a responsible Metaverse, is that those that share responsibility for the safety of users are usually the least familiar with the technologies and the ways in which people use them. This shared responsibility is greater than just between law enforcement agencies, and includes acknowledging (and ideally better defining through legislation) the responsibility and support needed for regulators, platforms and developers, parents, educators and users themselves. It is important to highlight how this shared responsibility is currently unevenly balanced, with a disproportionate amount falling onto parents and users - particularly young people, while platforms avoid accountability for the crimes occurring on their platforms, even when those crimes are enabled by the design choices made in their development.

The need to have greater digital literacy and experience in the Metaverse is most urgently needed with law enforcement. In order to offer the degree of protection required to ensure user safety, an understanding of how Metaverse platforms are designed and used is required and only achievable through more direct experience within those immersive environments. Lurking in the deepest, darkest parts of the Internet is not new for law enforcement, rather it is a key tactic for catching some of the worst crimes, namely in child sexual abuse cases. This approach has been necessary due to the increasing availability of end-to-end encryption, which prevents surveillance and oversight by law enforcement without being present in those spaces. With encryption becoming more prevalent - and also critically important for user safety at the same time - there will be an increasing need for law enforcement to be present in the Metaverse - and the resourcing required in achieving that is considerable.

DISRUPTION TACTICS IN THE METAVERSE

While litigation and prosecution of crimes online remain a priority in deterring future criminal activity and setting important precedents for regulators and law enforcement, success can be limited and delayed, resulting in further victims in the meantime. Disruption strategies are a key component for law enforcement in online crime because they sit within broader prevention approaches that obviously aim to stop potential harm before it occurs. For this reason, disruption tactics need to be prioritised by law enforcement seeking to police the Metaverse, and once again there are ample learnings from existing cybercrime initiatives. There are a wide range of strategies already in use including civil litigation, reducing the availability or highjacking of digital infrastructure, restricting access to funds, A.I. enabled anomaly detection, as well as undercover operations and account takeovers.

There are important ethical considerations in the use of these approaches, and often require close collaboration with the judiciary and platforms to ensure accountability and appropriate use. While previous and existing initiatives countering cybercrime offer numerous learnings and practices for policing the Metaverse, there is not a well established toolkit of disruption tactics to be leveraged and adapted for use in the Metaverse. This highlights the need for greater sharing of disruption practices, strategies and learnings between law enforcement agencies, to inform their replication and adaptation. Some of the disruption strategies discussed through the Think Tank include:

Website, Platform & Account Takeovers

Taking down accounts or websites conducting or hosting criminal activity has proven ineffective as perpetrators inevitably recreate accounts producing a game of 'whack-a-mole' for law enforcement. To counter this, law enforcement may infiltrate virtual spaces used by perpetrators by hijacking or taking over accounts and websites, enabling greater access to restricted or encrypted virtual spaces to gather intelligence and evidence. With this tactic used broadly, there is a need to establish and clarify the legal threshold for being granted a warrant to take over an account, and comes with significant ethical concerns that require oversight and accountability mechanisms. Examples of this takeovers include:

- Dutch police worked with a web-hosting firm to hijack and run Dark Web drug market, Hansa.
- Australian police ran and administered a known child abuse forum to identify perpetrators.
- The FBI and AFP seeded a fake encrypted messaging service into criminal networks to gather intelligence and evidence.

Digital Literacy

We consider digital literacy a disruption strategy in its own right. It is broadly accepted that there is a considerable gap between the number of actual incidents of cybercrime and those reported to authorities. This primarily is a product of a lack of awareness, concerns about having personal internet use exposed, and can vary significantly between age groups. It is well known that children in particular do not report when

they have bad experiences or are victimised online. Law enforcement requires reporting for referrals to kick start inquiries, and public reporting often leads to operations that deploy other tactics listed here.

A.I. Enabled Anomaly Detection

The use of A.I. technologies to detect anomalies and malware within systems is a well-used and successful tactic in cybercrime. There is significant potential for law enforcement to adapt these strategies to policing in the Metaverse, and requires further examination and testing to understand its use and ethical implications.

Targeting Digital Infrastructure

A significant number of cybercrime incidents are uncovered through strategic partnerships between law enforcement and the digital infrastructure that perpetrators and related-websites rely on - this can include web hosting firms, data servers and cloud storage providers, among others. This approach can require working relationships between those digital infrastructure providers and law enforcement - along with accountability to users. And is a form of indirect takedowns particularly useful when the target perpetrators are based in a jurisdiction that blocks access to law enforcement, but are usually reliant on supporting products that could be accessible.

Other Examples

Other strategies involve infiltrating digital infrastructure, tools and networks of perpetrators, like malware, web shells etc, to undermine cybercrime operations. This can include removing malicious programs and malware from computers to disrupt botnets, and removing backdoor access to computers and servers.

RECOMMENDATIONS

It is clear that law enforcement agencies require a refreshed approach to their operations and strategies to effectively police crimes in the Metaverse. This refreshed approach should strengthen existing strategies and coordination, and foster the development of new disruption tactics. Below are some key recommendations emerging from our Think Tank, for specific activities that such an approach should include - which should be informed by the following fundamentals:

- **Action-Oriented -** Incremental changes are constantly occurring to platforms and products, and law enforcement (as well as governments and regulators) need to not be caught on the back foot as many were in the internet 2.0 era. This means starting now to resource the training and digital literacy of law enforcement. Some participants framed this as a challenge of breaking free of the limitations of existing law enforcement culture that is shaped by 'what came before', in order to prioritise getting on with the job.

> *"Don't wait to ask for permission, disrupt it without permission of the industry, because they're not going to give you permission until things go extremely wrong"*
>
> *- Participant quote*

- **Not Wasting Time on Industry Permission -** There was broad acknowledgement of how slow many tech companies are resistant to mitigating crimes, and often will not take action until significant harm has occurred or after significant public pressure and scrutiny - often companies are more motivated by harm to their reputation or stock price over that of their users. Law enforcement should not be restricted by waiting for industry to take action - as is the broad expectation of the public.

- **Leaning into A.I. -** Greater consideration by law enforcement of the use of A.I. in detection and disruption of crimes is necessary in order to match the use of such technologies by perpetrators and organised crime online.

- **Innovation and Creativity -** Through both Think Tanks in this series, there was insightful discussion about the creativity of perpetrators and criminal groups in designing new ways of conducting their activities, as well as in avoiding detection. Co-designing with experts and users outside law enforcement could be a useful means to matching the innovation and creativity of perpetrators, for example exploring ways of bridging the gap between design thinking, policing and human rights.

> *"Creativity needs to infiltrate law enforcement culture in order to actually think of disruptive techniques"*
>
> *- Participant quote*

RECOMMENDATION 1:

Education, Training and Immersion For Law Enforcement

Investing in education, training and experience for law enforcement in the Metaverse will be critical to effectively reduce the prevalence of crimes in virtual environments. This capability building will not only familiarise law enforcement with the technologies and how they are used, but will also serve to support greater collaboration in the development of new disruption strategies. Alongside dedicated time within the Metaverse, this training should also include the following:

- **Research and Analysis -** In order to better understand the landscape, identify gaps and generate preventive strategies to the unknown dynamics of the Metaverse;
- **Collaboration -** For greater shared learnings across jurisdictions between agencies, which can also inform the development of regional frameworks;
- **Communications -** In order for law enforcement to more effectively communicate the threats and approaches to the public and policymakers.

RECOMMENDATION 2:

Establishing a Community Of Practice for Co-Designing Disruption Strategies

Given the lack of established disruption strategies for law enforcement in the Metaverse, we recommend the establishment of a Community of Practice for law enforcement that is action-oriented and focused on sharing insights and learnings, and co-designing disruption strategies for specific crimes or issues. During the Think Tank, there was one example provided by participants where a group of law enforcement, technologists and creatives were convened to workshop new strategies to a particular crime, which produced an out-of-the-box solution that is still in use today.

This Community of Practice could adopt a joint or global task force approach, that includes representatives from global, national and local agencies, with participation from other members of the community as needed, such as parents, educators, developers, young people, civil society, academics.

CONCLUDING REMARKS AND NEXT STEPS

It has been made abundantly clear that our law enforcement agencies are not adequately equipped to effectively police the Metaverse, and a significant amount of urgent action is required. We are extremely grateful to the participants of our Think Tanks and their valuable contributions, and we acknowledge that their interest and ongoing leadership on these issues is reliant on action from governments to get on with the task of legislating adequate enforcement powers and resourcing for law enforcement that are proportionate and work in the public interest.

This discussion paper is intended as a conversation starter, and we welcome further input and feedback on the themes and recommendations.

REFERENCES

Collier, K. (2023), 'FBI disrupts cybercrime operation by wiping malicious programs from hundreds of thousands of computers', NBC News, accessed 21 November 2023

Greenberg, A. (2018), 'Operation Bayonet: Inside the Sting that Hijacked an Entire Dark Web Drug Market', Wired, 8 March 2018

Hogan-Burney, A. & Ramsey, G. (2023), 'Cybercrime Disruption through Civil Litigation and Equitable Remedies', Lawfare, accessed 20 November 2023

Safi, M. (2016), 'The takeover: how police ended up running a paedophile site', The Guardian, accessed 21 November 2023

Tuffey, D. (2021), 'AN0M: How an app to decrypt criminal messages was born 'over a few beers' with FBI', Radio New Zealand, accessed 21 November 2023

U.S. Department of Justice - Office of Public Affairs (2021), 'Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities', published 13 April 2021

U.S. Department of Justice - Office of Public Affairs (2022), 'Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU)', published 6 April 2022

Victoria Police (2022), 'Cybercrime Strategy 2022-2027', accessed 21 November 2023