Background image: © *Iryna Dincer* | stock.adobe.com

AUSTIN C. DOCTOR, JOEL S. ELSON & SAMUEL T. HUNTER

# VIOLENT EXTREMISM, INNOVATION, AND RECRUITMENT IN THE METAVERSE

Austin, Joel, and Sam explore the interplay between trust-building, emerging technologies, and innovation, which can be used to help violent extremists enhance their recruitment techniques.

Like many recruiters, violent extremists have a growing interest and opportunity to exploit the metaverse to enhance their activities. Tapping into trust building mechanisms leveraged for centuries, traditional recruitment techniques will expand into new forms facilitated by digital capabilities. Using haptic feedback gloves, advanced robotics, and augmented reality devices, would-be recruiters will be able to shake hands, pour tea, and connect with potential members in ways previously only imagined. Understanding the interplay between trust-building, emerging technologies, and innovation offers useful insight into why this recruitment approach might work – and how this risk may be mitigated.

## WHAT IS THE METAVERSE AND WHY IS IT IMPORTANT TO RECRUITMENT?

Recent technological breakthroughs across computing disciplines are laying the foundation for a paradigm shift in how we experience and think about the internet. The metaverse is a term that is helpful in coalescing these divergent concepts into a single word that symbolises a future where the physical and virtual worlds are blurred beyond distinction. While building on disruptions brought about by the advent of the personal computer, the internet, and mobile devices, the enormity and impact of the metaverse across every aspect of human civilization could be unprecedented. The future of social, political, and economic engagement could well be transformed. Terrorism and violent extremism would be no exception.

As an interdisciplinary team of terrorism researchers at the National Counterterrorism Innovation, Technology, and Education (NCITE) Center in Omaha, Nebraska, we believe the metaverse offers fertile ground for exploitation through malevolent innovation. Although the metaverse affords violent extremist organisations increased capability across several fronts (e.g., planning, finance), we discuss recruitment as it is a precursor to many other malign activities.

> **...emerging technologies often leverage and amplify trust.**

## TRUST, INNOVATION, AND RECRUITMENT TO VIOLENT EXTREMISM IN THE METAVERSE

By design, emerging technologies often leverage and amplify trust. As referenced in a past issue of the *CREST Security Review*, trust is foundational for relationship building and recruitment, specifically. Drivers of trust come in several forms, with the consensus being that trust toward others is best depicted as a mix of the logical (cognitive) and emotional (affective).

Given the ubiquity of emerging technology, the ability for developers and users in the metaverse to provide such experiences that exploit our trust tendencies is rapidly on the rise. To illustrate the range of ways in which violent extremist recruiters might leverage trust and technology, consider the three following recruiters:

- Our first recruiter appears in a natural human form, but via the recruit's AR glasses they can subtly shift their appearance and presence. Their voice may be adjusted to be more authoritative, their physical appearance tailored to be more familiar, and their conversational tactics enhanced – all facilitating a stronger sense of connection and trust in the recruiter.
- Our second purely digital recruiter could optimise the environmental factors that facilitate trust building, by inviting the recruit to join in a completely virtual experience. An innocent collaborative game could be a carefully contrived experience designed to build trust, for example. For recruitment, the ability to not only discuss why their group may be worth joining but also showcasing what being a member would look like is a unique tool afforded by this approach.
- Our third recruiter, appearing as a human avatar that obscures the frame of a humanoid robot could facilitate trust not only through subtle cues in the digital overlay but also through direct manipulation of objects in the physical world. Such hybrid presence uniquely affords the opportunity for bringing an ingratiating gift to the meetup or placing a reassuring hand on one's shoulder. If done effectively, the experience will feel rich and connected, resulting in greater influence, persuasiveness, and trust.

## IMPLICATIONS FOR THE FRONT LINE

Violent extremists have an emerging opportunity to innovate by extending their recruitment practices into the metaverse. Their success will hinge on their ability to build trust in a blended digital-physical environment. This presents challenges and opportunities for practitioners, policymakers, and industry leaders.

The identification and implementation of any actionable solution will likely require focused coordination between corporations, policymakers, and law enforcement bodies. Even these may face some obstacles, however, as many such choices may mean making the metaverse less profitable in the near term, less immersive or organic to users, and/or more difficult to access.

There also remain valid practical concerns. For example, content moderation in the metaverse may be difficult to execute, especially as the digital and physical portions of the metaverse become increasingly fluid. And the legal infrastructure surrounding the metaverse remains weakly defined.

Extremists will continue to innovate, and the metaverse opens new opportunities for exploitation. While these risks are highly dependent on the rate and trajectory of the metaverse's development, we assess that the optimal window to proactively shape these factors is imminent, though handicapped by significant knowledge gaps. For the scientific and research-oriented communities, the development of effective and actionable solutions is contingent upon a clear conceptualization of the metaverse, a better understanding of how it will differ from existing analogues in form and function (e.g., online gaming, social media), and the evidenced anticipation of potential violent extremist tactics and techniques afforded by this new blended environment.

*Austin C. Doctor, Ph.D., is a political scientist at the University of Nebraska Omaha (UNO) and lead of counterterrorism research initiatives at the National Counterterrorism Innovation, Technology, and Education (NCITE) Center, a US Department of Homeland Security Center of Excellence. Joel S. Elson is an assistant professor of information technology innovation at UNO and lead of information science and technology research initiatives at NCITE. Sam Hunter, Ph.D. is a professor of organisational psychology at UNO and head of strategic operations at NCITE.*