## Potential Malign Uses of Extended-Reality Technologies

**SCOPE:** This product highlights potential uses of extended reality (XR) technologies by terrorist actors and offers considerations to public safety officials regarding this immersive virtual space. This product is not a response to a specific threat against the United States. It provides general awareness of, considerations for, and additional resources related to threats from international terrorists. This product uses the term "violent extremists" to refer to foreign violent extremists and those U.S.-based violent extremists who are directed, enabled, or inspired by, or who otherwise affiliate or collaborate with foreign violent extremists.

XR is a general term for a spectrum of technologies that integrates digital spaces and the real world, including virtual reality (VR) and augmented reality (AR), and are intended to provide different sensory and immersive experiences. XR is used to access the "metaverse" where users can interact with one another and aims to create an immersive experience using a multisensory display, blurring the lines between physical reality and the digital space. XR technology may present terrorists with potential opportunities to improve recruitment efforts by identifying, creating, and disseminating interactive messaging; to intimidate and threaten victims; and to refine tactics, techniques, and procedures (TTPs). XR technologies will expand these opportunities as they likely become smaller, faster, and more interconnected and provide an improved means of hiding one's true identity. Terrorists have historically leveraged technological developments, platforms, and applications and may use XR technologies to study, examine, and experiment.

The key differences in what XR technologies will offer from how we presently interact online are the concepts of presence and immersion—the feeling of being in the virtual space as opposed to looking at the virtual space through a screen.

- Terrorists may use XR technologies to conduct virtual training such as physiological desensitization by depicting graphic violence. Immersive technologies could make training more realistic and enhance the user's belief that the experience convincingly simulated a real-world interaction. These simulations could also provide more pathways to radicalization and mobilization to violence among vulnerable audiences.
- XR technologies can depict photorealistic and accurately scaled simulations of physical spaces and systems for locations such as banks, hospitals, schools, and government facilities. These simulations could provide users with opportunities to conduct robust and realistic training and attack planning while minimizing the risks of discovery.
- The anonymity provided by unregulated XR environments could foster permissive environments whereby violent extremist content can grow within virtual terrorist sanctuaries and enhance radicalization. For example, terrorists may use unregulated XR environments to create and interact with avatars of known terrorist figures or establish virtual training camps. This environment provides unique access and methods of targeting potentially vulnerable populations, particularly juveniles who may be susceptible to radicalizing based on violent extremist messaging.

### TRANSFORM

**Allows users to transform not only themselves but the virtual world that they inhabit. This can range from "avatars" to "locations" such as immersive and interactive environments.**

**This allows for training in stressful terrorism-related scenarios as well as improving officer skills, experience, and knowledge.**

### TRANSPORT

**Allows users to change the physical world around them up to and including full replacement.**

**Virtual replicas of crime scenes can be accessed and analyzed after the real-world scene has been altered. Conversely, they may be used by terrorists to study, memorize, and exploit.**

### TRANSCEND

**Allows users to create and participate in innovative AR, VR, and XR technologies; tools that tap into spatial reasoning and memory capabilities.**

**Spatial mapping can recreate a dynamic 3D map of the user's environment, allowing the device or user to understand the location and interact with the environment in the virtual world, offering law enforcement new investigative methods.**



NCTC-JFRT-2024-03166

5 NOVEMBER 2024
AUTHORED BY NCTC, DHS, FBI

# Considerations for Public Safety: Extended-Reality Technologies

Public safety agencies will likely find it challenging to detect, deter, and disrupt terrorists. The following considerations offer public safety partners recommendations on how to approach this problem as technology continues to evolve. Resources are listed to illustrate the variety of offerings and are not to be considered endorsements of the content or the material these organizations offer.

## COLLABORATION AND PARTNERSHIIPS

Collaboration with private-sector partners, including technology companies and community leaders, may improve methods to identify, interpret, and understand the various forms of terrorist activity occurring in XR environments. Enhanced partnerships may assist in the event of an exigent threat when information must be shared in a timely manner with platform and security officials.

Remain aware that multiple legal jurisdictions may be involved because of the global nature of these technologies. The evolving nature of emerging technology on a global scale often results in differences in laws and regulations, complicating investigative efforts. Increased familiarity with partner capabilities, authorities, and policies or procedures through collaborative environments provides opportunities to enhance incident and investigative responses.

Enhancing public awareness of reporting mechanisms and decreasing barriers that may reduce bystanders' willingness to report behaviors indicative of terrorism, such as concerns that their loved ones could be arrested, fears of being perceived as alarmists, fears of potentially slandering an innocent person, or negative perceptions of law enforcement, can provide opportunities for safe, secure, and accessible options to report and intervene if a person is radicalizing to violence. Consider public outreach efforts and educational opportunities such as hosting public town halls to help demystify the technology and improve the public understanding of radicalization to violence messaging.

## POLICY AND PLANNING

Develop and maintain guidance and legal processes to address terrorists' use of XR technologies. Knowledge of hardware or specialized tools may enable more expedient investigative processes.

Develop departmental policies that consider terrorist and other illicit uses of technologies. Update policies and guidelines to reflect continued growth and expansion of malicious actors' capabilities.

Remain up to date with terrorist TTPs and provide recurring training about emerging or developing technologies to counter potential exploitation. Consult with the local fusion center and the FBI Joint Terrorism Task Force to identify opportunities to share information and to request open-source reporting to aid in identifying potential terrorist threats or related activities before an event.

## INVESTIGATION

Digital forensics investigations involving XR technologies may include the collection of data, the recovery of deleted or hidden data, the analysis of data, the identification of potential witnesses of terrorist activity, the identification of potential witnesses of terrorist activity, the identification of an alleged attacker, and prevention. Investigations may involve multiple devices, networks, and platforms like social media websites and messaging applications and may include VR headsets and other wearables, computers, laptops, mobile phone(s), routers, and other smart devices.

Physical evidence, which is typically expected when investigating and adjudicating a case, may be lacking in investigations in which XR technology is used because they are virtual environments. Training of law enforcement, forensics specialists, cybersecurity professionals, and other officials may assist with the collection, analysis, and preservation of evidence required to apprehend and potentially prosecute terrorists.

Moderating terrorist activity, including recruitment, training, networking, and the spreading of violent extremist messaging, through XR technologies may become more challenging for law enforcement and security officials, especially as platforms and virtual spaces increase and physical locations in which observe or identify potential acts of terrorism decrease.

## ILLICIT FINANCING AND ASSOCIATED TECHNOLOGIES

Awareness of TTPs as well as the current threat landscape can help public safety officials identify terrorist connections that may be associated with XR technologies and illicit financing, improving the ability to respond to and mitigate threats.

Parts of some XR technologies utilize blockchain technology, like cryptocurrency, which may, under some circumstances, challenge law enforcement authorities' ability to interdict because of the decentralized and pseudonymous nature of transactions. Consequently, an awareness and understanding of transaction records, wallet addresses, and other digital artifacts on this technological platform may help identify patterns that indicate terrorism or other illicit activity.

A broad understanding of blockchain forensics and illicit cryptocurrency activities of funds derived from known suspicious or illicit sources, including ransomware attacks, darknet marketplaces, theft reports, or mixing or tumbling services, may provide observable indicators of terrorists using the technology.

Non-fungible tokens (NFTs) are unique forms of cryptographic assets which are bought and sold digitally on the blockchain and can be used across XR technologies. NFTs are represented by lines of code used to convey ownership of a good or asset, like digital art, that could be used by terrorists to launder illicit proceeds from criminal activities, evade sanctions, recruit, and disseminate terrorist messaging.

## RESOURCES

**INTERPOL: *Metaverse, A Law Enforcement Perspective, Use Cases, Crime, Forensics, Investigations, and Governance*** highlights investigative considerations including multi-jurisdictional impact and access and recovering evidence. www.interpol.int/content/download/20828/file/Metaverse%20%20a%20law%20enforcement%20perspective.pdf

**The Behavioral Threat Assessment Center (BTAC)** is FBI's lead for terrorism investigations related to threat assessment and threat management. BTAC conducts training and research and provides behaviorally based investigative and operational support, including case consultations, to law enforcement. BTAC's services can be requested by law enforcement through a local Behavioral Analysis Unit Threat Management Coordinator. https://www2.fbi.gov/hq/isd/cirg/ncavc.htm#bau

**The National Threat Evaluation and Reporting (NTER)** Program Office works collaboratively with federal, state, local, tribal, territorial, and private-sector partners to build the capacity to recognize the warning signs of terrorism and targeted violence, triage suspicious activity reporting, and address threatening or concerning behaviors before an individual escalates to violence. https://www.dhs.gov/nter

**JCAT First Responder's Toolboxes** may provide additional details to enhance understanding and assist with investigative efforts. Refer to the related First Responder's Toolboxes highlighted in each section for more detailed information, which can be found on JCAT's website, DHS's Homeland Security Information Network, or FBI's Law Enforcement Enterprise Portal.

- Emerging Technologies and Possible Malign Uses by Terrorists, July 2024
- Violent Extremists' Use of Generative Artificial Intelligence, May 2024
- Terrorist Exploitation of Online Gaming Platforms, October 2023
- Terrorists' Potential Use of Non-Fungible Tokens, February 2023
- Identifying and Preventing Terrorist and Other Illicit Financing, December 2022



NCTC-JFRT-2024-03166

5 NOVEMBER 2024
AUTHORED BY NCTC, DHS, FBI

JCAT

JOINT COUNTERTERRORISM ASSESSMENT TEAM

# PRODUCT FEEDBACK

**Please use the link below to complete a short survey. Your feedback will help JCAT develop counterterrorism products that support the public safety and private sector community.**

**https://www.JCAT-url.com**

For further information, please email JCAT
*jcat@odni.gov*

(U) The Joint Counterterrorism Assessment Team (JCAT) is a collaboration by NCTC, DHS, FBI, state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The First Responder's Toolbox is an ad hoc, unclassified reference aid intended to promote counterterrorism coordination among federal, state, local, tribal, and territorial government authorities and partnerships with private sector officials in deterring, preventing, disrupting, and responding to terrorist attacks.