Terrorist Exploitation of Online Gaming Platforms

Terrorists have used online gaming spaces to recruit, train, network, communicate, and spread terrorist messaging. Terrorist online gaming usage has included:

- Designing and producing video games that promote violent extremist narratives.
- Modifying (or "modding") existing video games to twist the narrative into a violent extremist message or fantasy.
- Using in-game chat functions to communicate with ideologically like-minded individuals and potential recruits.
- Using gaming-adjacent platforms[a] to convene like-minded individuals, socialize them to violent ideologies, and incite or mobilize them to violence.
- Using gaming references in messaging to normalize terrorist violence, terrorist symbols, or other violent extremist narratives, particularly among young audiences.
- Engaging in "gamification"—the use of gaming motivational techniques to encourage violence in nongaming contexts.

The online global gaming environment combines interactive gameplay with real-time conversations, creating individual and community relationships among users that might not otherwise exist outside these platforms, often in anonymous settings. This environment may provide opportunities to access terrorist or terrorist-related content through online gaming platforms and gaming-adjacent platforms like chat, resharing, or livestreaming features, particularly for juveniles who may be susceptible to extremist messaging. Insight into gaming technologies provides opportunities for public safety officials to enhance detection efforts, community outreach, and training to identify, mitigate, and respond to terrorist attacks.

- ISIS has used first-person-shooter video game perspective in recruitment videos that mimics footage from popular online games to reach a larger audience.
- Users have replicated and roleplayed prominent attacks in online games, including an attack in 2019 involving a racially or ethnically motivated violent extremist (RMVE) driven by a belief in the superiority of the white race who targeted two mosques in Christchurch, New Zealand.

CONSIDERATIONS: Collaboration with private sector partners and community actors, including technology companies and community leaders, may improve methods to identify, interpret, and understand the various forms of terrorist activity on gaming platforms. The following are some considerations for public safety officials in identifying and responding to potential terrorist threats from online gaming and gaming-adjacent platforms.

Identification and Awareness of Behaviors

- Be familiar with common or emerging online video gaming terminology to identify potential threats of violence and contextual behaviors that suggest a person could be mobilizing to violence. Code words may conceal identification and collection of potential threats. Partnerships with a variety of disciplines—including public safety, mental health, social service, faith, law enforcement, technology, and others—can help identify behaviors that could be concerning and provide resources to intervene.
- Remain cognizant that users may exploit a range of tactics to obfuscate threats posted on gaming and gaming-adjacent platforms by using emojis[b] or combinations of emojis and other indirect or ambiguous threat language intended to reveal threats of violence only to those familiar with the user, including references to "in-game" violence.
- Use risk assessment tools to identify and evaluate people exhibiting behaviors that could be concerning. Employ multidisciplinary teams to evaluate and communicate potential violent extremism threats, and develop and coordinate risk mitigation, supervision, and threat management options.

Law Enforcement Investigations

- Stopping livestreams during terrorism attacks is difficult, particularly during a rapidly evolving threat environment. Consider potential content derived from livestreamed attacks, which may provide valuable information to law enforcement and enhance investigative efforts especially during exigent circumstances.
- In the event of an attack, submit preservation letters to gaming companies, including game developers and game platforms, which may be separate entities. Submitting correct and relevant information in preservation requests is critical to ensuring timely and efficient responses.
- Be familiar with legal processes, applicable laws and policies, including civil liberty protections to collect and exploit data from online gaming platforms to supplement or enhance terrorism investigations. Refer to departmental policies and guidelines when conducting open-source research to identify threats, supplement investigations, and conduct official follow-up.
- Be aware that users may duplicate usernames across multiple platforms, which may provide critical insights into user and account details (e.g., emails, phone numbers) necessary during investigations. Enhanced open-source methodologies may identify potential terrorist threats, offer investigative leads, and supplement investigative efforts.
- Incorporate financial literacy into recurrent training and investigative protocols. Some online gaming platforms, which have a large global user base, allow for trading of virtual items and in-game currencies, which may even be traded for real currency outside the gaming environment, resulting in terrorism or other illicit activities.

SCOPE: This product is intended to raise the awareness of public safety officials about potential terrorist exploitation of online gaming systems or gaming-affiliated platforms. It highlights potential investigative resources, collaborative opportunities, and response considerations to terrorist threats from online gaming platforms.

ONLINE GAMING PLATFORM FUNCTIONS TERRORISTS MAY EXPLOIT

Gaming-affiliated communications	Platforms allow video game players to talk while gaming and may include text chat, file, and image sharing. Terrorists may use these platforms to communicate because they are often perceived as less moderated, less regulated, and anonymous.
Livestreaming and video platforms	Content creators can stream videos or post videos of attacks, which can provide terrorists instant notoriety and be used to incite further violence and follow-on attacks.
Digital distribution platforms	Also known as electronic marketplaces, enables users and developers to buy and sell video games and host user-generated content. Terrorists have developed first-person shooter video games designed to connect with like-minded individuals and promote violent extremist messaging.
Game and video consoles	Provide mainstream titles on personal computers, popular consoles, and niche web-browser games created by independent developers offering immersive interfaces that can enhance terrorist sympathizer's experience.
Financing and money laundering	Gaming and gaming-adjacent platforms may provide terrorists with loopholes to sell, trade, or exchange games, in-game items, and other gaming products in exchange for cryptocurrency or fiat money. Virtual currency exchanges often do not meet anti-money-laundering standards.

[a]Third-party applications that host large quantities of gaming content and communications that are distinctly separate from games. These applications expand access and social reach of the online gaming ecosystem.

[b]Digital image used to express an idea, emotion, object, or symbol.

NCTC-CO-2022-26517

24 OCTOBER 2023
AUTHORED BY NCTC, DHS, FBI

Terrorist Exploitation of Online Gaming Platforms *(continued)*

Public and Tech Sector Partnerships

- Distinguishing actual threats from violent gaming posts and references can be difficult. Enhance awareness of trends in terrorist online activity using open-source resources derived from the tech sector, academia, and civil society organizations.
- Participate in and contribute to cross-sector discussions with digital gaming moderators, tech sector officials, and other experts to build common understanding of terrorist iconography and lexicon used in gaming spaces.

GAMIFICATION OF VIOLENCE

- Gamification is the process of adding games or game-like elements to something (such as tasks) to encourage participation. Terrorists often use gamification to recruit, disseminate violent extremist messaging, connect, or engage with other like-minded individuals. It can also be used as an element in an attack where the attacker is the "designer" or "player" and other users on the platform are "spectators" or "observers."
- In May 2022, minutes before attacking a supermarket in Buffalo, New York, a RMVE who adhered to white supremist ideology and espoused a belief in the superiority of the white race, invited select members of their network to view a livestream of the attack. The attacker replicated the visual style of a first-person shooter game by wearing a helmet camera to film the attack, dressing in military-style combat gear, and using a long gun. A recording of the attack was posted online and viewed more than 600,000 times in less than 24 hours. Links to the video remained available through other gaming-adjacent platforms hours later. The alleged attacker is awaiting federal trial.

Processing Legal Requests to Gaming Platforms

- Investigators submitting preservation letters, subpoenas, search warrants, or other legal processes should ensure requests include the required identifying information or records and are submitted using the appropriate method to facilitate timely processing. The correctness of information submitted by law enforcement during legal processing may affect company response and the utility of information for law enforcement purposes.

PLATFORMS[c]	LAW ENFORCEMENT CONTACT FOR ROUTINE REQUESTS AND ADDRESS
Battle.net	**Company:** Blizzard Entertainment, Inc. **Contact:** custodianofrecords@blizzard.com **Address:** 16215 Alton Parkway, Irvine, CA 92618
Discord	**Company:** Discord, Inc. **Contact:** https://app.kodex.us/discord/signin **Address**: 444 De Haro St, Suite 200, San Francisco, CA 94107 **Note:** Process instructions found at https://discord.com/safety/360044157931-working-with-law-enforcement
Fortnite	**Company:** Epic Games, Inc. **Contact:** legal-response@epicgames.com **Address:** Box 254 2474 Walnut Street, Cary, NC 27518
Playstation Network	**Company:** Sony Interactive Entertainment LLC **Contact:** LE_legalrequests@playstation.sony.com **Address:** https://www.cscglobal.com/service/csc/csc-office-location **Note:** Process instructions found at https://www.search.org/resources/isp-list/
Roblox	**Company:** ROBLOX Corp. **Contact:** https://app.kodexglobal.com/roblox/signin **Address:** 970 Park Place, San Mateo, CA 94403
Steam	**Company:** Valve Software **Contact:** subpoenainquiries@valvesoftware.com **Address:** 10400 NE 4th Street, Suite 1400, Bellevue, WA 98004
Twitch	**Company:** Twitch Interactive, Inc. **Contact:** https://ler.amazon.com/us **Address:** 2710 Gateway Oaks Drive, Suite 150N, Sacramento, CA 95833 **Note:** More information found at https://safety.twitch.tv/s/article/Law-Enforcement-Response
Xbox Live	**Company:** Microsoft Corporation **Contact:** https://leportal.microsoft.com **Address:** Attn: Custodian of Records, 1 Microsoft Way, Redmond, WA 98052

[c]The information provided in this graphic includes contact information for some of the most popular gaming and gaming-adjacent platforms. It was gathered through open sources and should be verified before submitting to platforms.

[d]These materials and trainings are listed to illustrate the variety of offerings and are not to be considered endorsements of the content of the material or trainings these organizations offer.

RESOURCES[d]

- **Terrorism Online Tips** provides options to submit an anonymous tip to the FBI or other federal agencies, including DHS, the Federal Trade Commission, the Drug Enforcement Administration, the Internet Crime Complaint Center (IC3), the National Center for Missing & Exploited Children, and the Treasury Inspector General for Tax Administration. https://tips.fbi.gov/; https://www.tigta.gov
- **DHS–Center for Prevention Programs and Partnerships** seeks to prevent targeted violence and terrorism by working with the whole of society to establish and expand local prevention frameworks. https://www.dhs.gov/CP3
- **Department of State Global Engagement Center** coordinates the US Government's efforts to recognize, understand, and counter foreign state and nonstate efforts aimed at undermining or influencing the policies, security, or stability of the United States. https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/
- **Tech Against Terrorism** collaborates with the public sector to provide the global tech industry resources to combat terrorist use of the internet. https://www.techagainstterrorism.org/about/
- **Global Internet Forum to Counter Terrorism** is an NGO aimed at preventing terrorists from exploiting digital platforms. https://gifct.org/
- **Global Network on Extremism & Technology** seeks to prevent terrorist exploitation of technology. https://gnet-research.org/
- **International Center for Digital Threat Assessment**, "Raising Digitally Responsible Youth" https://resources.saferschoolstogether.com/view/474771331/

NOTE: Many of the activities described herein may involve constitutionally protected activities and may be insignificant on their own. Action should not be taken solely based on the exercise of constitutionally protected rights. These gaming platforms are primarily used for lawful, protected communication, and use of these platforms alone is not an indicator that a person is likely to be a terrorist.

NCTC-CO-2022-26517

24 OCTOBER 2023
AUTHORED BY NCTC, DHS, FBI

JOINT COUNTERTERRORISM ASSESSMENT TEAM | JCAT

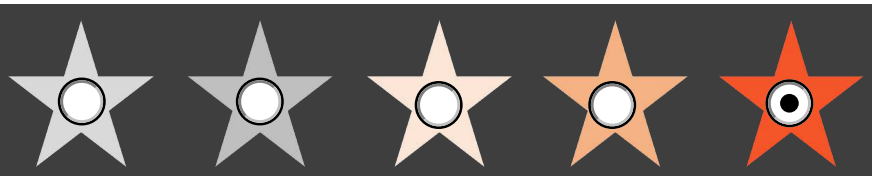
PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and ORG:

DISCIPLINE: ☐ LE ☐ FIRE ☐ EMS ☐ HEALTH ☐ ANALYSIS ☐ PRIVATE SECTOR DATE:

PRODUCT TITLE: Terrorist Exploitation of Online Gaming Platforms

POOR  GREAT

ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS.

WHAT TOPICS DO YOU RECOMMEND?

SUBMIT