Project craaft
Collaboration, Research & Analysis Against the Financing of Terrorism

This publication is supported by: The NATO Science for Peace and Security Programme

Virtual Threats: Terrorist Financing via Online Gaming

Gonzalo Saiz

Research Briefing No. 1

About Project CRAAFT

Project CRAAFT is a research and community-building initiative aimed at strengthening global counter-terrorist financing (CTF) efforts. The initiative began with CRAAFT I and continues with CRAAFT II – Collaborative Responses to the Role of New Technologies in Terrorist Financing – launched in 2025. This new phase focuses on how emerging technologies impact terrorist financing and is led by the Centre for Finance and Security (CFS) at RUSI, in partnership with RUSI Europe and the Regional Institute for Security Studies (RISS) in Tbilisi. The project is supported by the NATO Science for Peace and Security (SPS) Programme. Learn more at <projectcraaft.eu>

The views expressed in this publication are those of the author, and do not reflect the views of RUSI or any other institution.

The observations made in this research briefing reflect the views of the author only; they should not necessarily be regarded as reflecting NATO views or policy.

Published in 2025 by the Royal United Services Institute for Defence and Security Studies.

Introduction

The global popularity of the video game industry attracts billions of users to its platforms. However, with a vast and diverse audience, these entertainment platforms can also draw in problematic characters and have become a target for abuse by terrorists and extremists. This exploitation has drawn significant academic and regulatory attention to the need for content moderation – to curb the spread of extremist propaganda, and to curtail terrorist recruitment efforts within the gaming sector.[1]

Terrorists and extremists have participated extensively in the gaming space through a range of activities. They have developed their own video games, modified mainstream games to introduce extremist elements, and made use of in-game communication functions and gaming-adjacent platforms.[2] Through these activities, extremist actors have extended the reach of their propaganda and recruitment initiatives to a larger audience (beyond their local community or country). These activities also have the potential to serve as funding opportunities for violent actors.

Despite extensive study into extremist behaviours online, including within the gaming sector, the financing possibilities and related risks around the terrorist and extremist milieus in video games remain largely understudied. This briefing will contribute to expanding the counterterrorist financing (CTF) literature by exploring the following areas through a financial lens: the regulation of the gaming industry, in-game purchases, the production of bespoke games and modifications, the risks associated with communication functions in gaming and gaming-adjacent platforms, and emerging risks within the intersection of gaming and terrorist financing.

Regulation in the Video Gaming Space

Approximately 3.4 billion people worldwide played video games in 2024.[3] The global video game market generated $187.7 billion in revenue in 2024 and is projected to reach $213.3 billion by 2027.[4] Despite its vast scale, much of the financial crime risk in this market remains unaddressed.

Regulatory efforts have primarily focused on combating the spread of extremist content, propaganda, and recruitment activities within gaming platforms. However, money laundering and terrorist financing risks have not received the same attention.[5] The Second[6] and Third[7] EU Anti-Money Laundering Directives (AMLD), and the subsequent directives, targeted money laundering and terrorist financing in online gambling but did not extend similar scrutiny to online gaming.[8] Additionally, the Fifth AMLD excluded from its scope in-game virtual currencies

[1] Council of the European Union, 'Online Gaming in the Context of the Fight Against Terrorism', 6 July 2020, <https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf>, accessed 22 April 2025; Linda Schlegel, 'Extremists' Use of Gaming (Adjacent) Platforms: Insights Regarding Primary and Secondary Prevention Measures', Radicalization Awareness Network, 2021, <https://home-affairs.ec.europa.eu/system/files/2021-08/ran_extremists_use_gaming_platforms_082021_en.pdf>, accessed 22 April 2025; Suraj Lakhani, Jessica White and Claudia Wallner, 'The Gamification of (Violent) Extremism: An Exploration of Emerging Trends, Future Threat Scenarios, and Potential P/CVE Solutions', Radicalization Awareness Network, 2022, <https://home-affairs.ec.europa.eu/gamification-violent-extrrmism-exploration-emerging-trends-future-threats-scenarios-and-potential_en>, accessed 22 April 2025; Galen Lamphere-Englund and Jessica White, 'The Online Gaming Ecosystem: Assessing Digital Socialisation, Extremism Risks and Harm Mitigation Efforts', Global Network on Extremism and Technology (GNET), May 2023, <https://gnet-research.org/2023/05/26/the-online-gaming-ecosystem/>, accessed 22 April 2025; Jessica White et al. 'Radicalisation through Gaming: The Role of Gendered Social Identity', *RUSI Whitehall Report*, 2-24 (December 2024).

[2] There is no common definition of gaming platforms or gaming-adjacent platforms. In this briefing, gaming platforms are defined as those that offer users the possibility of playing specific video games. Gaming-adjacent platforms are external apps where users do not play, but rather interact with each other for gaming-related communications. Online gambling – related to betting and games of chance – is a separate industry with a different set of risks. Online gambling thus falls outside the scope of this paper.

[3] Michiel Buijsman, 'The Global Games Market Will Generate $187.7 Billion in 2024', *Newzoo*, 13 August 2024, <https://newzoo.com/resources/blog/global-games-market-revenue-estimates-and-forecasts-in-2024>, accessed 15 September 2024.

[4] *Ibid.*

[5] Council of the European Union, 'Online Gaming in the Context of the Fight Against Terrorism'.

[6] Council of the European Union, 'Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 Amending Council Directive 91/308/EEC on Prevention of the Use of the Financial System for the Purpose of Money Laundering', *Official Journal of the European Union* (L344, 28 December 2001).

[7] Council of the European Union, 'Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing', *Official Journal of the European Union* (L309/15, 26 October 2005).

[8] Council of the European Union, 'Online Gaming in the Context of the Fight Against Terrorism'.

that are limited to their specific gaming environments, and that cannot be exchanged for fiat currencies.[9]

The Fifth AMLD does, however, regulate providers involved in exchanging virtual currencies for fiat currencies. Certain convertible in-game currencies that can be exchanged for fiat currency could fall under the scope of the directive. As Anton Moiseienko and Kayla Izenman argue, 'whether a currency or commodity is valuable depends on whether people treat it as such', and 'if in-game items can be traded, officially or unofficially, there is a strong argument that they meet the FATF's [Financial Action Task Force] virtual asset definition' and thus fall within the purview of AML/CTF regulation.[10]

At the operational level, monitoring and screening transactions within gaming and gaming-adjacent platforms also face significant challenges. Often, these platforms rely on payment service providers facilitating transactions to conduct due diligence on their users. Financial institutions have access to more reliable identifying data than gaming platforms, which frequently lack Know Your Customer controls.[11] Yet, the lack of regulation creates the risk that this responsibility is shifted between both parties. This 'pass the buck' effect undermines effective oversight and heightens the risk of terrorist financing going undetected within the gaming industry.

The very label of 'terrorist financing' is limiting in this regard. The latest reports from the FATF[12] and Europol[13] increasingly use the term 'violent extremism' to highlight the risks posed by actors that are not yet designated as terrorists. However, the blurred lines between terrorism and extremism further complicate the monitoring responsibilities of obliged entities under CTF regulations and of platforms seeking to mitigate related risks. The uncertainty around potential obligations to target activities and narratives from designated terrorist entities, from extremists that promote violence, or from extremists whose opinions may or may not be related to violence, undermines the effective monitoring of relevant risks that might fall beyond a narrow understanding of the CTF scope. For this reason, this briefing covers relevant fundraising initiatives in the gaming space by both terrorist and extremist actors.

In-Game Purchases

Many mainstream online video games feature in-game transactions, known as microtransactions, allowing players to buy and sell in-game items, upgrades, cosmetic enhancements and other content using fiat currency. This capability raises concerns about the potential for criminals to launder the proceeds of crime through these unregulated channels. Instead of transferring funds via traditional bank transfers or common payment services like PayPal, users can transfer equivalent amounts through valuable in-game items. These items can be sold within the game, or on adjacent platforms, and cashed out in fiat or cryptocurrency.

Research into the financial crime risks of in-game purchases has revealed significant money laundering concerns. In 2018, Valve, the owner of the digital game distributor Steam, reported that almost all microtransactions in the game 'Counter-Strike: Global Offensive' were part of money laundering operations.[14] Similarly, research indicated that criminals worldwide abused Fortnite's virtual economy during the same year.[15]

A common method for laundering money through in-game purchases involves a criminal buying in-game currency or items with a prepaid or stolen card. The criminal then sells

[9] *Ibid*.

[10] Anton Moiseienko and Kayla Izenman, 'Gaming the System: Money Laundering Through Online Games', *RUSI Newsbrief* (Vol. 39, No. 9, October 2019).

[11] Mavis Bennett, 'The Potential Perils of Online Gaming', *ACAMS Today*, 8 June 2023, <https://www.acamstoday.org/the-potential-perils-of-online-gaming/>, accessed 13 June 2024.

[12] Financial Action Taskforce (FATF), 'Ethnically or Racially Motivated Terrorism Financing', FATF Report, June 2021, <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Ethnically-racially-motivated-terrorism-financing.html>, accessed 22 April 2025.

[13] Europol, *European Union Terrorism Situation and Trend Report 2023 (TE-SAT)* (Luxembourg: Publications Office of the European Union, 2023), <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat>, accessed 22 April 2025.

[14] Matthew Gault, '"Nearly All" Counter-Strike Microtransactions are Being Used for Money Laundering', *Vice*, 29 October 2019.

[15] Anthony Cuthbertson, 'How Children Playing Fortnite are Helping to Fuel Organised Crime', *The Independent*, 13 January 2019.

the in-game currency or items via a third-party platform, often at prices below market value, to attract buyers.[16] Additionally, some online games also offer 'loot boxes', which are 'gambling-style microtransactions that facilitate the collection of randomly selected in-game artefacts whose contents are only revealed to the buyer after purchase'.[17]

The money laundering risks of in-game purchases are substantial. Indeed, valuable virtual items could potentially provide a stream of revenue for some extremist actors that possess them. However, while microtransactions present attractive opportunities for criminals seeking to launder money, they appear to be less enticing for terrorist financiers. Scarce evidence of such abuse currently exists and disrupting such activities without clear pre-existing extremist indicators on the users involved would be challenging.[18] Nonetheless, the potential for these virtual economies to be exploited for financial crimes underscores the need for vigilant monitoring and regulation in the gaming industry.

Sale of Extremist Games and Modifications

Terrorists and extremists across the ideological spectrum will go to great lengths to spread their message and engage in fundraising activities. Among these efforts is the production of original video games to disseminate their ideologies, an activity that was particularly popular in the early 2000s[19] but continues to present day.[20] Groups such as Hezbollah developed games like 'Special Forces' in 2003 and 'Special Force 2: Tale of the Truthful Pledge' in 2006, where players can impersonate Hezbollah fighters and combat the Israeli military. Right-wing extremist groups also created similar games. The white supremacist organisation National Alliance released 'Ethnic Cleansing' in 2002, allowing players to control a Ku Klux Klan member or a neo-Nazi skinhead during the so-called race war. The game sold for $14.88,[21] referencing the '14' and '88' numbers commonly used in right-wing extremist milieus.[22]

While the scale of production might have declined over the decades, terrorist and extremist groups continue to release and sell new bespoke games. In more recent examples, Hezbollah itself released a new video game, 'Holy Defence' in 2018, where users could play as Hezbollah members to fight the Islamic State (IS).[23] In 2019, 2GenPro (also known as 2Genderz Productions) released 'Jesus Strikes Back: Judgment Day,' where players could shoot members of the LGBTQ+ community using extremist figures as avatars. One of the available avatars included Brenton Tarrant, who killed 51 people in a shooting in a Christchurch, New Zealand mosque. The game also sold for $14.88.[24] 2GenPro have continued producing similar video games, including a sequel, 'Jesus Strikes Back 2: The Resurrection', 'Simp Slayer Simulator 2K20', and 'Blackpill Bill: God's Work'. 2GenPro sold these video games in promotions at $39.99 for an eight-game bundle.[25]

[16] Moiseienko and Izenman, 'Gaming the System'.

[17] *Ibid.* It is worth noting that across the EU, there are different national interpretations of whether loot boxes should be regulated as gambling activities. See Dentons, 'Loot Box Regulation in the EU – Loading Status', 28 June 2023, <https://www.dentons.com/en/insights/guides-reports-and-whitepapers/2023/june/28/loot-box-regulation-in-the-eu-loading-status>, accessed 13 June 2024.

[18] Author interview with law enforcement official dedicated to counter terrorist financing (CTF), online, September 2024.

[19] Suraj Lakhani, 'Video Gaming And (Violent) Extremism: An Exploration of the Current Landscape, Trends, and Threats', *Radicalisation Awareness Network*, 2021.

[20] Emily Thompson and Galen Lamphere-Englund, '30 Years of Trends in Terrorist and Extremist Games', Global Network on Extremism and & Technology, November 2024, <https://gnet-research.org/wp-content/uploads/2024/10/GNET-47-Extremist-Games_web.pdf>, accessed 13 November 2024.

[21] See the screenshots of the website retrieved from *Archive Today*, 'Ethnic Cleansing: The Game', <http://web.archive.org/web/20020215223748/http://www.resistance.com/ethniccleansing/catalog.htm>, accessed 26 June 2024.

[22] 1488 is a popular combination of white supremacist numeric symbols. 14 is shorthand for David Lane's '14 Words' slogan: 'We must secure the existence of our people and a future for white children'. 88 stands for 'Heil Hitler' (H being the eighth letter of the alphabet). See Anti-Defamation League, '14/88', Hate on Display, General Hate Symbols, Numeric Hate Symbols, <https://www.adl.org/resources/hate-symbol/1488>, accessed 22 April 2025.

[23] Michael Barak, '"Holy Defense" – Hezbollah's New Computer Game', *International Institute for Counter-Terrorism*, March 2018, <https://ict.org.il/holy-defense-hezbollahs-new-computer-game/>, accessed 22 April 2025.

[24] See here the screenshots of the 2GenPro website retrieved from Archive Today, '2GenPro', <https://archive.ph/Uo5h3>, accessed 26 June 2024.

[25] *Ibid.*

Kvltgames, an Austria-based video game developer financially backed by the German far-right identitarian organisation Ein Prozent,[26] produced 'Heimat Defender: Rebellion' in 2020. The game is reportedly free to download, and Ein Prozent claimed that it reached 20,000 downloads within the first week.[27] A second game, called 'The Great Rebellion', was released in February 2024 and was also partially financed by Ein Prozent. It is still available for purchase on Steam for $15.99,[28] and has generated an estimated gross revenue of $94,500.[29] It currently has over 400 individual reviews. Alex Jones, founder of American far-right conspiracy theorist outlet Infowars, also launched a game for $17.76 – in a nod to the 1776 American Declaration of Independence – that is also currently available for purchase.[30] The game is estimated to have raised $318,000.[31]

Extremist games and mods often make headlines, but their role as a profitable fundraising stream for extremists remains uncertain.

Even recent events have been gamified, such as the Hamas attacks on 7 October 2023, which can be reenacted in 'Fursan al-Aqsa: The Knights of the Al-Aqsa Mosque'. The developer promoted the game at a discounted price of $7, available on Steam via Reddit from April 2024.[32] The game's gross revenue is estimated at $67,900.[33]

Aside from the creation of bespoke games, many mainstream video games also allow user modifications (mods), which extremists have notoriously abused. Sandbox games such as Roblox and Minecraft, where users can build their own interactive worlds and minigames, are frequently flagged for the introduction of extremist motifs (including recreations of the Christchurch shooting).[34] The Daily Stormer, a right-wing extremist news site, released a modification of 'Doom 2', where players fight a Jewish World Conspiracy.[35] IS supporters have also 'modded' popular games like 'Grand Theft Auto' (GTA) and 'Call of Duty' (CoD),[36] and modifications made to the game 'Arma III' allowed users to play from the perspective of the terrorists.[37] While most mods are available to download for free, their appeal in extremist milieus makes them a potential source of revenue that should be monitored.

But revenue does not only come from game and mod sales; it also comes from donations during the gameplay. In October 2023, Nick Fuentes, a prominent American right-wing extremist, hosted a livestreamed fundraiser tournament in the game 'Fortnite' and raised over $163,000 for the America First Foundation.[38]

Extremist games and mods often make headlines, but their role as a profitable fundraising stream for extremists remains uncertain. They are often removed from digital distribution services like Steam and represent a significant investment for the creators.[39] Still, recent research estimates revenue figures from the sale of extremist games in Steam range between $15,000 and $500,000.[40] Furthermore, the continued

[26] Göksel Türker and Ali Gök, 'Video Games and Radical Movements: "Ein Prozent" and "Heimat Defender"', *Journal of Strategic Security* (Vol. 17, No. 2, 2024), pp. 89–125.

[27] Tim Hume, 'A German Far-Right Group is Trying to Recruit Kids with a Free Video Game', *Vice*, 21 September 2020, <https://www.vice.com/en/article/germany-game-heimat-defender-identitarian/>, accessed 29 April 2025.

[28] Steam, 'The Great Rebellion', <https://store.steampowered.com/app/2732820/The_Great_Rebellion/>, accessed 29 April 2025.

[29] Thompson and Lamphere-Englund, '30 Years of Trends in Terrorist and Extremist Games'.

[30] Global Project Against Hate and Extremism, 'How the Far-Right Spreads Hate Through Gaming', 31 January 2024, <https://globalextremism.org/post/how-the-far-right-spreads-hate-through-gaming/>, accessed 22 April 2025.

[31] Thompson and Lamphere-Englund, '30 Years of Trends in Terrorist and Extremist Games'.

[32] Reddit, 'Fursan al-Aqsa: The Knights of the Al-Aqsa Mosque', <https://en.wikipedia.org/wiki/Fursan_al-Aqsa:_The_Knights_of_the_Al-Aqsa_Mosque>, accessed 23 June 2024.

[33] Thompson and Lamphere-Englund, '30 Years of Trends in Terrorist and Extremist Games'.

[34] Cecilia d'Anastasio, 'How Roblox Became a Playground for Virtual Fascists', *Wired*, 10 June 2021, <https://www.wired.com/story/roblox-online-games-irl-fascism-roman-empire/>, accessed 29 April 2025.

[35] Council of the European Union, 'Online Gaming in the Context of the Fight Against Terrorism'.

[36] Lamphere-Englund and White, 'The Online Gaming Ecosystem'.

[37] Nick Robinson and Joe Whittaker, 'Playing for Hate? Extremism, Terrorism, and Videogames', *Studies in Conflict & Terrorism*, 11 January 2021, pp. 1–36.

[38] America First Foundation, <https://americafirstfoundation.org/>, accessed 5 May 2025; *Ibid.*

[39] Radicalisation Awareness Network, 'Extremists' Use of Video Gaming – Strategies and Narratives', Conclusions Paper, 9 November 2020, <https://home-affairs.ec.europa.eu/system/files/2020-11/ran_cn_conclusion_paper_videogames_15-17092020_en.pdf>, accessed 22 April 2025.

[40] Thompson and Lamphere-Englund, '30 Years of Trends in Terrorist and Extremist Games'.

accessibility of many of these games, and the disposition of users to pay for this content, present significant risks that should be addressed more effectively by authorities and relevant platforms. This is particularly relevant in the case of donations solicited during livestreaming gameplays, which can amount to high-volume financial flows. This is addressed in further detail in the next section.

Gaming for Communication and Financial Exploitation

As extremists are increasingly pushed off mainstream social media platforms due to stricter content moderation, many have migrated to gaming and gaming-adjacent communication platforms and have now become popular venues for extremists to connect and communicate.[41]

All major online video games – such as CoD and GTA, and gaming platforms like PlayStation Network, Xbox Live, and Steam – feature in-game voice communication and chat rooms with varying degrees of encryption. These functions provide extremists with potential avenues for disseminating propaganda and engaging in recruitment efforts. Although instances of extremists making first contact via in-game chat are rare, they are not unprecedented. IS supporters have suggested using in-game chats in mobile games to recruit and incite lone-actor attacks.[42] This same in-game voice and text chat functions can provide terrorists and extremists with relatively secure platforms to solicit donations and provide guidance on how to conduct financial transactions securely to avoid detection. Extremists can target users on these open platforms and then invite them to more private and secure environments for further communications.

According to a survey of 2,200 people across seven countries, approximately 16% of gamers were solicited for donations by extremist groups or individuals on a gaming platform.[43] Players can use gaming-adjacent platforms, like Twitch, Discord and Mumble, which support text and video chat. For example, users can host livestreams on a similar platform and explicitly solicit donations in a voice- and video-recorded format from their audience. Users can also request audience members to transfer the funds to a PayPal account, a crypto wallet or using the platform's own digital currency. DLive, another live-streaming platform, has faced these issues, with extremists soliciting donations, answering paid questions, and promoting merchandise using DLive's own blockchain-based cryptocurrency architecture.[44] Alternatively, extremists could (in theory) raise funds from advertisements on the platform, from paid subscriptions or sponsorships.[45] This could also be done in writing, through chats or forums like Discord, as well as through non-gaming platforms like 4chan.

Australia's financial intelligence unit, AUSTRAC (the Australian Transaction Reports and Analysis Centre), identified 104 far-right and ideologically motivated violent extremism channels on Bitchute (a video content platform). These channels use various funding methods, including Bitchute's tipping function; using online money transfer services and virtual assets (31 of 104 channels); hosting links to crowdsourcing and subscription-based channels like Patreon (49 of 104 channels), and Subscribestar (19 of 104 channels); and hosting links to DLive, which has a payment function that allows users to tip a channel via virtual assets.[46] Media reports indicate that many top-earning channels on DLive promote white supremacist theories and conspiracy theories, with top channels earning between $150,000 and $550,000 in 2020.[47]

In the first half of 2024, Discord took action against 17,567 distinct accounts for violent extremism, including disabling 16,309 accounts and removing 2,607 servers.[48] Discord has been used for planning offline events, such as the Unite the Right rally in Charlottesville, Virginia, in August 2017. Organisers used Discord to plan and promote the

[41] Schlegel, 'Extremists' Use of Gaming (Adjacent) Platforms'.

[42] Council of the European Union, 'Online Gaming in the Context of the Fight Against Terrorism'.

[43] White et al. 'Radicalisation Through Gaming'.

[44] Schlegel, 'Extremists' Use of Gaming (Adjacent) Platforms'.

[45] *Ibid*.

[46] FATF, 'Crowdfunding for Terrorist Financing', October 2023, <https://www.fatf-gafi.org/en/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html>, accessed 22 April 2025.

[47] Hannah Gais and Michael Edison Hayden, 'Extremists are Cashing in on a Youth-Targeted Gaming Website', Southern Poverty Law Center, 17 November 2020, <https://www.splcenter.org/resources/hatewatch/extremists-are-cashing-youth-targeted-gaming-website/>, accessed 29 April 2025.

[48] Discord, 'Discord Transparency Report: January –June 2024', 1 November 2024, <https://discord.com/safety-transparency-reports/2024-h1>, accessed 13 November 2024.

event within overtly extremist servers such as the 'National Socialist Army' and 'Führer's Gas Chamber'.[49]

The crackdown on extremism has led these groups to become more discreet in their online activities and fundraising efforts. It is increasingly difficult for investigators to identify extremist milieus that have toned down or completely disguised their ideologies to avoid detection.[50] Extremist groups use less moderated, less regulated, and more anonymous gaming communication systems as a teaser to then share radical content on more secure platforms.[51]

In that regard, the majority of these gaming platforms offer their players mechanisms to report content, which can later be identified and removed by the operator.[52] Although text chat is easier to analyse, voice chat poses additional challenges for content moderation. For this reason, some investigators fear a lack of knowledge of the real figures around terrorist financing in the gaming sector.[53] There are some initiatives to introduce AI voice chat moderation, which some platforms and games, like CoD, are deploying.[54] However, a greater understanding of the risks is needed to address these emerging threats effectively.

Emerging Risks in New Gaming Spaces

The gaming industry is constantly evolving with the development and introduction of new technologies. The emergence of blockchain technologies, the growing presence of virtual assets, and new platforms where these items would converge (such as the 'Metaverse'[55]) might alter the threat landscape.

These emerging platforms enable digital identification and proof of ownership, the collection of digital assets such as non-fungible tokens (NFTs), and cryptocurrency transfers. Access to the Metaverse will likely require individuals to own a cryptocurrency wallet to hold their digital assets, potentially increasing the use of virtual assets. While this might entail more money laundering than terrorist financing risks, some opportunities might arise for terrorist and extremist actors.

These developments might open avenues to continue traditional fundraising methods in a virtual format. Right-wing extremist actors most commonly raise funds through membership fees, and through commercial activities such as concerts, mixed-martial arts fights and merchandise sales. All these activities could be taken to the virtual world, including sales of membership tokens (allowing buyers to join the virtual community), fundraising through the sale of NFTs featuring extremist symbols, and organising online concerts or avatar fights within the Metaverse. This form of decentralised financing could enable terrorist organisations to develop their own online ecosystems, potentially creating their own Metaverses with unique currencies for value transfer purposes or mere marketing.[56]

Although the Metaverse might offer more opportunities for money laundering than terrorist financing, the integration of virtual assets to access exclusive games and chatrooms presents additional risks. These spaces can become less transparent and more exclusive, providing more opportunities for illicit activities to escape regulatory scrutiny. Therefore, it is crucial to monitor these emerging platforms to prevent the misuse of advanced technologies for terrorist financing and other criminal activities.

Conclusions

The gaming industry is a highly active and profitable sector, with a vast and diverse user base spread across numerous games and platforms. This complexity poses significant

[49] Kevin Rose, 'This Was the Alt-Right's Favorite Chat App. Then Came Charlottesville', *New York Times*, 15 August 2017.

[50] Author interview with law enforcement official dedicated to CTF, online, April 2024.

[51] Council of the European Union, 'Online Gaming in the Context of the Fight Against Terrorism'.

[52] *Ibid.*

[53] Author interview with law enforcement official dedicated to CTF, online, September 2024.

[54] Call of Duty, 'Anti-Toxicity / Disruptive Behavior Progress Report – Moderation Results and Readiness for Black Ops', 10 October 2024, <https://www.callofduty.com/blog/2024/10/call-of-duty-anti-toxicity-progress-report-black-ops-6-moderation-results>, accessed 13 November 2024.

[55] The metaverse can be defined as a 3D-enabled digital space that uses virtual reality, augmented reality and other technology to interact with the virtual world. However, there is no standard definition of the metaverse. See Simon Brawley, 'What is the Metaverse and What Impacts Will it Have for Society?', UK Parliament Post, 19 July 2024, <https://post.parliament.uk/research-briefings/post-pb-0061/>, accessed 22 April 2025.

[56] Council of the European Union, 'The Metaverse in the Context of the Fight Against Terrorism', Special Report, 2 June 2022, <https://data.consilium.europa.eu/doc/document/ST-9292-2022-INIT/en/pdf>, accessed 22 April 2025.

challenges for regulation and monitoring of the industry. While the gaming space has been extensively studied to curtail the proliferation of propaganda and recruitment efforts, the financial risks attached to this industry remain understudied and underregulated.

Online gaming presents substantial money laundering risks, particularly through in-game transactions and the convertibility of in-game items into fiat currency and cryptocurrencies. Although terrorist and extremist actors do not typically use online games for the transfer or storage of funds, as traditional criminals do, they have engaged in producing and selling bespoke games that occasionally produce considerable amounts of revenue.

A larger risk is emerging from terrorist and extremist actors raising donations through livestreamed gameplays in gaming and gaming-adjacent platforms. Most importantly, these platforms may provide secure and unregulated communication channels, especially in voice and video formats, allowing extremists to solicit donations and potentially instruct supporters on how to conduct transactions without detection.

Increased law enforcement scrutiny has led extremist actors to be more discreet in their fundraising efforts within gaming platforms, where they already benefit from the enhanced privacy levels these platforms offer. This trend raises concerns about the lack of knowledge regarding the actual volume of terrorist financing occurring within the online gaming industry.

To better understand and address these risks, the FATF should conduct a sectoral risk analysis of the gaming industry. This could involve disseminating a survey among its members and tasking the Risk, Trends, and Methods Working Group with producing a bespoke report. The European Commission should also assess the risks of money laundering and terrorist financing in online gaming in its next report on AML/CTF risks affecting the internal market and cross-border activities, as previously recommended by the Council of the European Union.[57]

The outcome of this sectoral risk analysis would determine whether expanding AML/CTF regulations to cover the gaming industry would offer tangible benefits to strengthen the CTF response. Clarifying the responsibilities between gaming platforms and payment service providers, and ensuring effective user and transaction screening, would mark effective first steps. Additionally, introducing reporting mechanisms could enhance investigators' understanding, by allowing them to operate within a regulated space (supported by intelligence that has been submitted by the obliged entities). However, the regulation of the gaming industry must be proportionate and risk-based.

As online gaming continues to evolve rapidly, so too will the threat landscape. The EU and national authorities must develop a nuanced understanding of this space and its emerging risks – to stay ahead of the curve and prevent further abuses by terrorist and extremist financiers.

About the Author

Gonzalo Saiz is a Research Fellow at the Centre for Finance and Security at RUSI, focusing on sanctions and counter threat finance. As part of Project CRAAFT, his research focuses on counter threat finance, including the use of new technologies for terrorist financing, abuse of NPOs, crime-enabled terrorist financing, and financing of right-wing extremism. His research also covers sanctions implementation, circumvention and evasion tactics, and sanctions enforcement. He leads the research of SIFMANet (Sanctions and Illicit Finance Monitoring and Analysis Network).

[57] Council of the European Union, 'Online Gaming in the Context of the Fight Against Terrorism'.