



Global Network
on Extremism & Technology

The Online Gaming Ecosystem: Assessing Digital Socialisation, Extremism Risks and Harms Mitigation Efforts

Galen Lamphere-Englund and Jessica White

May 2023

*GNET is a special project delivered by the International Centre
for the Study of Radicalisation, King's College London.*

The authors of this report are Galen Lamphere-Englund and Jessica White. This report is a product of the Extremism and Gaming Research Network.

W: <https://extremismandgaming.org/>

Twitter: @ExtremismGaming

LinkedIn: <https://www.linkedin.com/company/egrn/>

The Global Network on Extremism and Technology (GNET) is an academic research initiative backed by the Global Internet Forum to Counter Terrorism (GIFCT), an independent but industry-funded initiative for better understanding, and counteracting, terrorist use of technology. GNET is convened and led by the International Centre for the Study of Radicalisation (ICSR), an academic research centre based within the Department of War Studies at King's College London. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing those, either expressed or implied, of GIFCT, GNET or ICSR.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**

E. **mail@gnet-research.org**

Twitter: **[@GNET_research](https://twitter.com/GNET_research)**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.

© GNET

Recommended citation:
Lamphere-Englund, Galen, and Jessica White.
"The Online Gaming Ecosystem: Assessing Socialisation, Digital Harms, and Extremism Mitigation Efforts." Global Network on Extremism and Technology (GNET), May 2023.
<https://doi.org/10.18742/pub01-133>.

Executive Summary

This report provides a review of the research on the exploitation of gaming and gaming-adjacent platforms by violent extremists and the policies seeking to mitigate the impact of that exploitation. There is increasing interest in the nexus of online gaming and (violent) extremism. This report builds on the work of the Extremism and Gaming Research Network (EGRN) to provide a primer for those new to this space and an updated state of play of the cutting-edge research taking place among members of the network and beyond.

The report is divided into three sections.

First, it lays out the online gaming ecosystem. The report identifies gamers, the unique individual and community identity formations that can happen in these spaces and the multifaceted environment in which this takes place, including games, gaming-adjacent spaces and beyond.

Second, it builds upon and enhances a typology of potential harms in the online gaming ecosystem. This typology allows clarification of the different ways in which extremism can both spread through these spaces and how extremists can specifically exploit these spaces and communities.

Third, it provides an overview of some of the efforts that are currently ongoing to mitigate these potential harms. This includes efforts in the tech industry to reinforce policies and moderation efforts, by game designers to address potential challenges at an early stage and by practitioners who use online gaming engagement or gamification to prevent and counter violent extremism effectively.

Finally, the report concludes by looking to the future of this exponentially expanding space. It offers some recommendations for research, policy and practice to better understand and address the threat of extremism within online gaming to protect and enhance online gaming as a positive engagement space.

Contents

Executive Summary	1
<hr/>	
1 Introduction	5
<hr/>	
2 The Online Gaming Ecosystem	7
Gamers and Their Communities	7
The Online Gaming Environment	10
<hr/>	
3 Typology of Extremist Harms	15
Creating New Video Games and Modifications	15
Gamification for Radicalisation	17
Exploiting Gaming as Pop Culture	19
Exploiting Online Games for Communication	19
Exploiting the Gaming Environment and Adjacent Platforms	20
Financing and Money Laundering	20
<hr/>	
4 Mitigating Extremist Harms to Gaming Spaces	23
Trust and Safety Efforts	23
Safety by Design	24
Positive Interventions	24
Gamifying Prevention Initiatives	25
<hr/>	
5 Conclusion: Looking to the Future	27
Recommendations	27
<hr/>	
Policy Section	31

1 Introduction

Violent extremist and terrorist groups actively exploit video games and the digital platforms around them.¹ While researchers have not found a direct line of causation between violence in video games and offline violence,² there is evidence indicating that far-right extremists in the United States, Germany and New Zealand have livestreamed attacks on platforms built for watching video games,³ created social networks on gaming-adjacent platforms to mobilise for violence⁴ and designed their own games.⁵ Violent jihadist groups also recruit through gaming platforms,⁶ create propaganda with video game themes⁷ and develop bespoke games.⁸ It is more important than ever to understand who, how, where and why online gaming and gaming-adjacent spaces are being used and abused by extremist actors. At the same time, it is essential to emphasise that online gaming environments provide overwhelmingly positive and pro-social experiences for most users.

As our lives become exponentially more intertwined with technology, online games provide a window into interactive virtual realities – or metaverses – to come. As such, online denizens, policymakers and tech creators must understand the potential risks and take collective steps to build resilience against exploitation by violent extremist and terrorist actors. Therefore, this report builds on the work of the Extremism and Gaming Research Network (EGRN) over the last two years to provide an up-to-date overview for policymakers, tech sector practitioners and newcomers to the latest research into the nexus of extremism, radicalisation and gaming, as well as a primer on the online gaming ecosystem for those unfamiliar with the space.

In 2021, the EGRN was established better to understand the risks and exploitation occurring in games and across gaming platforms. The Network exists to bring together researchers in this space, grow the evidence base and translate knowledge and lessons learned from preventing and countering violent extremism (P/CVE) to the gaming

-
- 1 Anti-Defamation League (ADL), "Hate Is No Game: Hate and Harassment in Online Games 2022," www.adl.org, 2022; Galen Lamphere-Englund and Luxinaree Bunmathong, "State of Play: Reviewing the Literature on Gaming & Extremism" (Extremism and Gaming Research Network (EGRN), 2021; 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" (Radicalisation Awareness Network (RAN), 2022).
 - 2 APA Task Force on Violent Media, "Technical Report on the Review of Violent Video Game Literature," 2015.
 - 3 Suraj Lakhani and Susann Wiedlitzka, "'Press F to Pay Respects': An Empirical Exploration of the Mechanics of Gamification in Relation to the Christchurch Attack," *Terrorism and Political Violence*, 31 May 2022, 1–18.
 - 4 Rachel Kowert, Alexi Martel, and William B. Swann, "Not Just a Game: Identity Fusion and Extremism in Gaming Cultures," *Frontiers in Communication* 7 (17 October 2022); Jacob Davey, "Gamers Who Hate: An Introduction to ISD's Gaming and Extremism Series," Institute for Strategic Dialogue (ISD), 2021; Daniel Koehler, Verena Fiebig, and Irina Jugl, "From Gaming to Hating: Extreme-Right Ideological Indoctrination and Mobilization for Violence of Children on Online Gaming Platforms," *Political Psychology*, 28 August 2022, <https://doi.org/10.1111/pops.12855>.
 - 5 Anti-Defamation League, "Hate Is No Game"; Nick Robinson and Joe Whittaker, "Playing for Hate? Extremism, Terrorism, and Videogames," *Studies in Conflict & Terrorism*, 11 January 2021, 1–36.
 - 6 Singapore Ministry of Home Affairs (MHA), "Issuance of Orders under the Internal Security Act against Two Self-Radicalised Singaporean Youths," Ministry of Home Affairs, 21 February 2023, <https://www.mha.gov.sg/mediaroom/press-releases/issuance-of-orders-under-the-internal-security-act-against-two-self-radicalised-singaporean-youths/>.
 - 7 Firas Mahmoud, "Playing with Religion: The Gamification of Jihad," Danish Institute of International Studies (DIIS), 27 September 2022, https://pure.diis.dk/ws/files/9007170/The_gamification_of_jihad_DIIS_Report_2022_06.pdf; Cori E. Dauber, Mark D. Robinson, Jovan J. Baslious, and Austin G. Blair, "Call of Duty: Jihad – How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos," *Perspectives on Terrorism* 13, no. 3 (2019): 17–31, <https://www.jstor.org/stable/26681906>.
 - 8 Linda Schlegel, "Jumanji Extremism? How Games and Gamification Could Facilitate Radicalization Processes," *Journal for Deradicalization*, no. 23 (24 June 2020): 1–44.

industry and policy. At its inception, the EGRN published a review of existing research on these topics,⁹ highlighting the current state of play at the time. The report highlighted several knowledge gaps ranging from the need to understand games as communication channels, to better researching socialisation processes leading to radicalisation on gaming platforms and identifying methods for “curbing extremist behaviour and radicalisation through gaming-based interventions”.¹⁰ Those gaps shaped the goals of the EGRN and have been the focus of its efforts over the last two years. This has resulted in several answers to the initial questions as to how gaming and extremism overlap.

Thus, this report builds upon the initial review of the literature to highlight the learnings of the EGRN and its members and to capture the cutting-edge research that is currently being done on the nexus of extremism and online gaming. This report first outlines the online gaming ecosystem and its makeup, then lays out a typology by which to think about the scope and variety of the potential extremism and radicalisation concerns, and finally highlights existing efforts to increase the safety of the online gaming environment.

⁹ Lamphere-Englund and Bunmathong, “State of Play”.

¹⁰ *ibid.*, 16.

2 The Online Gaming Ecosystem

To understand how extremists exploit the online gaming ecosystem, we first need to understand who gamers are, how their communities form, how they interact and the online gaming environment inside which they operate. Online gaming has become the most prominent entertainment sector. Around three billion people play video games – a number that soared during lockdowns prompted by the coronavirus pandemic – and by 2025 another 500 million people will be gaming.¹¹ Global revenues for 2022 are expected to generate \$184.4 billion, dwarfing film, television and music.¹² Revenues are anticipated to continue to grow year on year as the number of players increases. As this industry asserts itself as the dominant entertainment and engagement sphere, it is vital that we better understand this space, including the potential positive and negative impacts it has directly on those playing, as well as on society more broadly.

Gamers and Their Communities

People who play games are more diverse than ever and are no longer mostly male. Some 48% of players in the United States are women, while the average player is 33 years old.¹³ Most tend to start young and continue playing throughout their lives: 71% of American children play video games, while 65% of adults do. A quarter (24%) of people playing games in the USA are under 18, 36% are between the ages of 18 and 34, and some 40% are 35 or older.¹⁴ While global demographics are harder to estimate, most gamers appear to fall into similar cohorts. As a younger audience, gamers are often part of a prime recruitment demographic for armed groups and violent extremist organisations worldwide.¹⁵ Globally, the highest share of gamers is in the Asia-Pacific region (1.75 billion people, or around 55%), followed by the Middle East and North Africa (MENA) with 488 million and Europe with 430 million.¹⁶ The fastest growing audiences are in MENA and Latin America, growing, respectively, 8.2% and 4.8% annually.¹⁷

Social Spaces and Identity Formation

Non-gamers often misunderstand online gaming as a solitary activity that is inherently anti-social. However, this report situates games and gaming-adjacent spaces – especially online ones – as a) social spaces and b) generally beneficial experiences. The social dynamics of this ecosystem serve a powerful purpose, with often very positive

11 Newzoo, "Newzoo Global Games Market Report 2022," Newzoo, 26 July 2022.

12 Newzoo, "The Games Market in 2022: The Year in Numbers," Newzoo, 2022.

13 Entertainment Software Association (ESA), "Essential Facts about the Video Game Industry 2022," July 2022. <https://www.theesa.com/wp-content/uploads/2022/06/2022-Essential-Facts-About-the-Video-Game-Industry.pdf>.

14 *ibid.*

15 Gudrun Østby, Siri Aas Rustad, Roos Haer, and Andrew Arasmith. "Children at Risk of Being Recruited for Armed Conflict, 1990–2020." *Children & Society*, 15 July 2022. <https://doi.org/10.1111/chso.12609>.

16 Newzoo, "Newzoo Global Games Market Report 2022," Newzoo, 26 July 2022.

17 *ibid.*

effects. While games are entertainment media, they also possess distinct ‘gamer’ culture – and subcultures – associated with them. These gaming communities and subcultures can have very positive socialisation impacts and increase personal feelings of belonging, life satisfaction and self-esteem.¹⁸ However, equally and oppositely, as with real-world peer group dynamics, these spaces can have negative influences and they can contribute to anti-social behaviour and leave individuals vulnerable to radicalisation and recruitment.

Social spaces inside the online gaming environment, like any community, create opportunities for exploitation and harm.¹⁹ Exploration of gamer identities and their resilience and vulnerabilities to online extremism continues to be a topic of investigation for members of the EGRN, along with the unique socialisation dynamics of the online gaming environment. Pro-group behaviour is often socialised and built upon ‘othering’, which has been identified as a potential contributor to the use of online gaming spaces as recruitment avenues for extremist ideologies. Othering is a key process in identity-building that occurs by stigmatising those who do not share similar characteristics, ideas or values and thus do not belong to the in-group of the community.²⁰ Through this, an opposition of us versus them is created, which is in turn used to construct or reinforce a stronger individual identity.²¹ It is possible that in-game content and socialisation within the online gaming ecosystem can contribute to othering.²²

For example, it is possible that the propagation of toxic masculinity in gamer cultures has left online gaming spaces more vulnerable to radicalisation than other online spaces. This can be seen with the popularity of the misogynistic #GamerGate movement demonstrating how gamer cultures and identities have the potential to cultivate extreme pro-group behaviour.²³ #GamerGate, a hashtag most popular in 2014 and 2015 but continuing to have an impact today, is an online harassment campaign that began as a targeted campaign against a female journalist who was writing on diversity and progressivism within the online gaming space, but turned into a wide-scale radical right and misogynist backlash against those deemed not to fit the ‘traditional’ male gamer profile. The online gaming environment has long been defined by the male-dominated game design industry and has historically discouraged or been oblivious to the diversity of gamers and gamer identities. Another example is in realistic war games and often-powerful biases in their depiction of the enemy, which may resonate negatively with players belonging to that nationality.

18 M. Cwil, and W. T. Howe, “Cross-cultural analysis of gamer identity: A comparison of the United States and Poland,” *Simulation & Gaming* 51 (6) (2020), 785–801; W. Howe, D. Livingston, and S. K. Lee, “Concerning gamer identity: An examination of individual factors associated with accepting the label of gamer” (2019); L. K. Kaye, R. Kowert, and S. Quinn, “The role of social identity and online social capital on psychosocial outcomes in MMO players,” *Computers in Human Behavior* 74 (2017), 215–23.

19 Rachel Kowert, “Dark Participation in Games,” *Frontiers in Psychology*, 10 November 2020, <https://www.frontiersin.org/articles/10.3389/fpsyg.2020.598947/full>; Jessica White, “Community and Gender in Counter-Terrorism Policy: Challenges and Opportunities for Transferability Across the Evolving Threat Landscape,” *International Centre for Counter-Terrorism Journal*, <https://www.icct.nl/publication/community-and-gender-counter-terrorism-policy-challenges-and-opportunities>.

20 Yasmin Saikia and Chad Haines, *On Othering*, University of Chicago Press, 2023.

21 Martin Buber *Between Man and Man* (Translated by Ronald Gregor Smith), London: Collins, 1961.

22 Karen Lumsden and Emily Harmer, *Online Othering: Exploring Digital Violence and Discrimination on the Web*, Cham, Switzerland: Palgrave Macmillan, 2019.

23 For more on Gamergate, see Emily St. James, “#Gamergate: Here’s why everybody in the video game world is fighting,” *Vox*, 13 October 2014; Jay Hathaway, “What Is Gamergate, and Why? An Explainer for Non-Geeks,” *Gawker*, 10 October 2014; and Evan Urquhart, “Gamergate Never Died,” *Slate*, 23 August 2019.

When video games reflect a particular ethnocentric view of the world, they marginalise those who do not share the same fundamental characteristics or beliefs, which can lead to the formation of alternative communities based upon in-group/out-group identities.²⁴

Whether based on ethnicity, gender, sexual orientation or other identity factors, this type of othering and the formation of strong peer in-group/out-group influences within gaming culture present significant opportunities for extremists to infiltrate gaming culture. Additionally, those strong group dynamics and affirmative social bonds create the potential to increase risks of radicalisation.²⁵ When one aspect of identity – being a gamer, in this case – overwhelms other complex layers of identity, individuals are more likely to support their gamer group above all else. This sort of identity fusion, through which the group identity becomes internalised, has been shown by researchers both to provide a deep sense of belonging and to increase the risk of individuals heading down pathways of radicalisation.²⁶ Gamer identity fusion has been shown to be correlated with extremist views, a willingness to fight and die for other gamers and a host of other concerning psychological indicators, including psychopathy.²⁷

Community Definition and Formation

Just as online gamers are more diverse than ever, so are their communities. While we often hear reference to the ‘online gaming community’ as though it is a singular organism, it is essential to remember that this ecosystem supports myriad communities. These collectives form in different ways and their sense of communal identity can be grounded in divergently shared factors. While the conception of communities historically has often revolved around shared physical spaces (for example, neighbourhoods or religious/community centres, sports fields and so on), the transnational nature of online spaces allows for the formation of communities across physical and linguistic barriers, among others. It also provides a potentially more accessible engagement space for those who find real-world social interaction challenging.

While online gaming communities are (usually) initially formed around gameplay, they often extend into the formation of social bonds beyond simply gaming interactions. For most players, games and the communities around them are extraordinarily beneficial. Beyond just entertainment, online video games provide stress relief and creative problem-solving opportunities and serve as social

24 Kowert et al. (2022); Rachel Kowert, Presentation for Extremism and Gaming Research Network, 2021.

25 Scott Atran and Jessica Stern, "Small Groups Find Fatal Purpose through the Web," *Nature* 437 (7059) (September 2005): 620, <https://doi.org/10.1038/437620a>; Scott Atran, *Talking to the Enemy*. Harper Collins, 2010; Logan Molyneux, Krishnan Vasudevan, and Homero Gil de Zúñiga, "Gaming Social Capital: Exploring Civic Value in Multiplayer Video Games," *Journal of Computer-Mediated Communication* 20 (4) (9 May 2015): 381–99, <https://doi.org/10.1111/jcc4.12123>.

26 Ángel Gómez, Juana Chinchilla, Alexandra Vázquez, Lucía López-Rodríguez, Borja Paredes, and Mercedes Martínez, "Recent Advances, Misconceptions, Untested Assumptions, and Future Research Agenda for Identity Fusion Theory," *Social and Personality Psychology Compass* 14 (6) (23 April 2020), <https://doi.org/10.1111/spc3.12531>; Ángel Gómez, Alexandra Vázquez, Lucía López-Rodríguez, Sanaz Talaifar, Mercedes Martínez, Michael D. Buhrmester, and William B. Swann, "Why People Abandon Groups: Degrading Relational vs Collective Ties Uniquely Impacts Identity Fusion and Identification," *Journal of Experimental Social Psychology* 85 (November 2019). <https://doi.org/10.1016/j.jesp.2019.103853>.

27 Rachel Kowert, Alexi Martel, and William B. Swann, "Not Just a Game: Identity Fusion and Extremism in Gaming Cultures," *Frontiers in Communication* 7 (17 October 2022), <https://doi.org/10.3389/fcomm.2022.1007128>.

spaces where people from all walks of life can interact.²⁸ The sense of community in multiplayer games keeps players engaged and provides social bonds and interaction. Similarly, borders between interactions in virtual and physical spaces are increasingly fluid, with the experiences in games increasingly thought to be deeply impactful or even real.²⁹ While the debate is heating up now about what the metaverse should look like, gamers have lived in virtual worlds for years. Immersive, social experiences have long existed in games, from the 25-year-old fantasy title *Ultima Online* to the 20-year-old virtual world *Second Life*.³⁰ However, the impacts of these socialisation and community experiences will only increase with the growing prevalence of online activity and increasingly higher numbers of gamers.

The Online Gaming Environment

The gaming environment encompasses a dizzying array of genres, platforms and activities. For gamers, engagements range from playing specific games to watching livestreams of influential gamers who offer a running commentary while playing their favourite titles, to playing in competitive esports tournaments,³¹ to posting on forums, image boards and review sites dedicated to games.

The games market, for example, is divided into mobile games (responsible for around 53% of revenue globally last year), console games, including the Xbox and PlayStation (27%), PC games played on computers (19%) and in-browser games (1%).³² Inside those different categories, the actual games vary enormously.

Our research primarily focuses on multiplayer games, as these allow users to play and interact with others online. However, many games are single-player and do not offer opportunities to engage with other players. Genres and their associated risks also vary enormously. Venerable First Person Shooters (FPS) like *Call of Duty* and *Counterstrike* make headlines, while newer FPS franchises like the world's most popular game, *Fortnite*, and other popular titles like *Apex Legends*, are massive revenue drivers. However, the stunning profitability of blockbuster or AAA titles, as top-selling games are called, comes alongside ongoing reports of hate speech, harassment and extremist content in gaming settings. At the same time, nine of 14 leading gaming companies in the USA have made no public efforts to assess or mitigate extremist content in their products.³³

28 Linda K. Kaye, Rachel Kowert, and Sally Quinn, "The Role of Social Identity and Online Social Capital on Psychosocial Outcomes in MMO Players," *Computers in Human Behavior* 74 (September 2017): 215–23; Entertainment Software Association (ESA), "Essential Facts about the Video Game Industry 2022," July 2022, <https://www.theesa.com/wp-content/uploads/2022/06/2022-Essential-Facts-About-the-Video-Game-Industry.pdf>.

29 David Chalmers, *Reality+: Virtual Worlds and the Problems of Philosophy*, W. W. Norton, 2022.

30 John-Clark Levin, "Welcome to the Oldest Part of the Metaverse," *MIT Technology Review*, 17 February 2023.

31 Short for 'electronic sports', esports are an online gaming translation of popular real-world sports, often taking the form of organised, multiplayer competitions.

32 Newzoo, "The Games Market in 2022: The Year in Numbers," Newzoo, 2022.

33 Lori Trahan, "Summary of Responses from Gaming Companies," U. S. House of Representatives, February 2023, https://trahan.house.gov/uploadedfiles/summary_responses_to_letter_game_companies_online_harassment_extremism.pdf.

The gaming environment extends beyond games to include gaming-adjacent platforms, esports, forums, hardware manufacturers and even cultural references and publications. As with the various types of games, the risks and harms from extremist actors and content vary across the different environments. The gaming environment primarily consists of the following:

Type	Key Actors / Examples
Game studios/ developers	Riot Games, Epic Games, Blizzard Entertainment (now Activision-Blizzard)
Game publishers	Activision Blizzard, Sony Interactive Entertainment, Tencent Games, Nintendo, Microsoft, Valve Corporation, Take-Two Interactive, Bethesda Softworks, Electronic Arts (EA), Ubisoft
Game markets	Steam, GOG.com, itch.io, GameFly, Xbox, Epic Games Store, Green Man Gaming, Kinguin
Livestreaming platforms	Twitch, YouTube Live/YouTube Gaming, Facebook Watch/Facebook Gaming, Instagram Live, TikTok Live, Younow, DLive, Trovo, Steam
Video platforms	YouTube, Netflix, Vimeo, Ustream, Dailymotion, Dtube, PeerTube, Odysee, Lbry, Bitchute
Gaming forums and messaging platforms	Discord, Reddit (r/gaming), IGN Boards, Minecraft Forum, GameFAQ, Steam, 4Chan, 8Kun, Kiwifarms
Gaming publications, review sites and user-generated mod-servers	PCGamer, The Verge, Edge Magazine, MetaCritic, ModNexus
Esports teams and sports	Team Liquid, OG, FaZe Clan, Team Spirit, G2 Esports
Hardware manufacturers	Nvidia, Intel, AMD, Oculus, Asus, Razer, Alienware/Dell

Chart one: the gaming environment.

The gaming industry and ecosystem may seem immense to those unfamiliar with it, thus making it useful to contextualise the problem of extremism and radicalisation inside the scale of the sector. In communities comprising three billion players and as violent extremist organisations actively seek to propagandise, recruit and organise online, a degree of harmful and extremist content should be expected. However, while genuine risks and harms are occurring in gaming and gaming-adjacent platforms, these should not be generalised to all gamers, games or platforms.

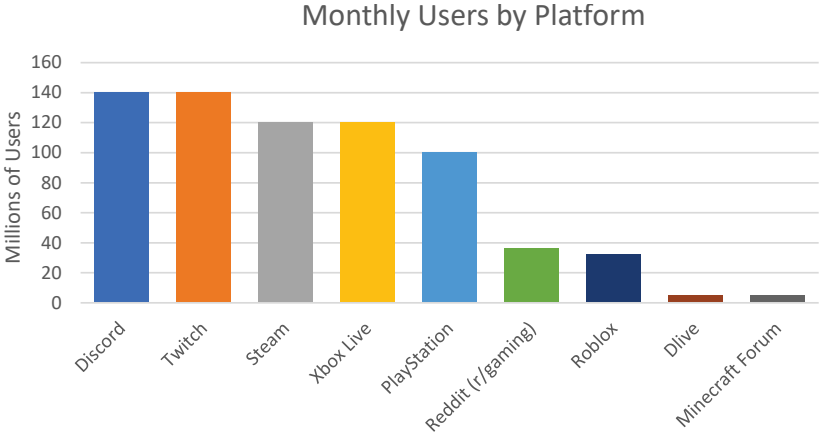


Chart two: monthly users of gaming and gaming-adjacent platforms (Data compiled by Statista, 2022).

Community behavioural norms within games vary tremendously: FPS titles like *Call of Duty*, *Grand Theft Auto* and *Valorant* rank among the primary places where players encounter white supremacist extremist content.³⁴ Sandbox games such as *Roblox* and *Minecraft*, where users can build their own interactive worlds and mini-games, are also regularly flagged for extremist content.³⁵ Nonetheless, real-time strategy (RTS) games are not often called out by researchers for direct exploitation by extremist communication, but far-right actors take advantage of historical gameplay to create alternative realities and downloadable game content based on white supremacist ideologies. Other genres, such as sports and racing titles like *Mario Kart* or *FIFA*, puzzle games, role-playing games (RPGs) like *The Witcher*, or massive multiplayer online role playing games (MMORPGs) like *World of Warcraft*, seem to have comparatively little specific extremist content.

34 Anti-Defamation League, "Hate Is No Game".
 35 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/>; Rachel Kowert, Austin Botelho, and Alex Newhouse, "Breaking the Building Blocks of Hate," Anti-Defamation League (ADL), 1 July 2022, https://www.adl.org/sites/default/files/pdfs/2022-07/ADL_CTS_Minecraft%20Content%20Moderation%20Report_072622_v2.pdf; Martin Seng, "'Roblox' und Rechtsextremismus: Das Kinderspiel mit Nazicontent," *www.zeit.de*, 19 February 2023, <https://www.zeit.de/digital/games/2023-02/roblox-rechtsextremismus-gaming-kinder-inhalte/seite-2>; Singapore Ministry of Home Affairs (MHA), "Issuance of Orders under the Internal Security Act against Two Self-Radicalised Singaporean Youths," Ministry of Home Affairs, 21 February 2023, <https://www.mha.gov.sg/mediaroom/press-releases/issuance-of-orders-under-the-internal-security-act-against-two-self-radicalised-singaporean-youths/>.

White-Supremacist Extremist Experiences, by Game

Share of people who reported experiencing white-supremacist extremism in the following games, by age group

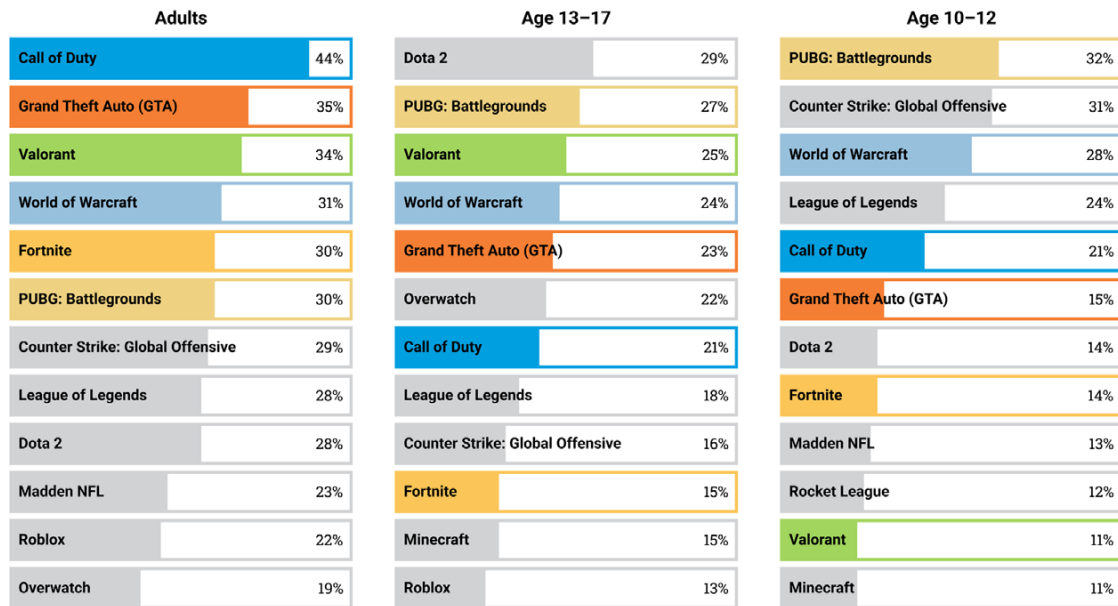


Chart three: from “Hate is No Game: Hate and Harassment in Online Games 2022”, ADL, 2022.³⁶

In addition to community behavioural norms, it is essential to understand the spectrum of potential threats within the online gaming ecosystem fully. Elements such as game design, content and community moderation (or lack thereof) and safety by design principles must be explored. Each of these may increase or decrease vulnerability to use or abuse by bad actors. As this is a highly diverse market, we should not assume that extremist content and risks are equally present across all games and platforms.

³⁶ ADL, “Hate Is No Game: Hate and Harassment in Online Games 2022” (ADL, 2022), <https://www.adl.org/sites/default/files/documents/2022-12/Hate-and-Harassment-in-Online-Games-120622-v2.pdf>.

3 Typology of Extremist Harms

To simplify the spectrum of potential threats, the EGRN has been working to devise and augment a typology of potential harms. The Radicalisation Awareness Network (RAN) created a framework for assessing how “video games and gaming adjacent communication platforms and gaming imagery [are used] by violent extremists” in 2020.³⁷ The EGRN has since built upon this and expanded it into a six-part revised typology of the ways in which extremist and terrorist actors use games and gaming-adjacent platforms.³⁸ Importantly, we can think of the extremist logic as being either:

- **organic**, as extremists innately use gaming as “as a means of bringing already radicalised people together”;³⁹ or
- **strategic**, as violent extremist organisations directly co-opt gaming tactics or platforms for their ends.⁴⁰

The six categories of typology of potential harms and even the two types of extremist logic often overlap, reflecting the hybrid nature of extremist activities online. However, these can provide a helpful framework through which to understand the threat environment.

Creating New Video Games and Modifications

Terrorists and extremists create their own video games. In 1999, the Columbine school shooters in the USA designed their own maps of their school in *Doom* prior to perpetrating a massacre, bringing games onto the radar of extremist groups. Since 2002, when a white supremacist hate group designed a standalone antisemitic game entitled *Ethnic Cleansing*, various actors have regularly produced extremist games. The EGRN has documented over thirty extremist or terrorist-related games and mods, though there are likely significantly more. Some of these are full titles that require users to find the game online, download and install it, and then slog through a (typically) poorly designed game. Others modify existing games – what is known as a “mod” – allowing users to stay in familiar gaming environments while accessing extremist narratives and imagery. For example, white supremacist and far-right groups have produced a relatively popular range of Deus Vult mods for games dating from the 1990s shooter *Doom* to more current strategy titles, including *Medieval II* and *Hearts of Iron IV*. Recently, extremist users or sympathisers in sandbox games like *Roblox* and *Minecraft* have built re-enactments of far-right rallying icons, like the Christchurch terror attack and Nazi internment

37 Radicalisation Awareness Network (RAN), “Extremists’ Use of Video Gaming - and Narratives” (Radicalisation Awareness Network (RAN), 11 September 2020)

38 Lamphere-Englund and Bunmathong, “State of Play”.

39 Davey, “Gamers Who Hate”.

40 Linda Schlegel, “Extremists’ Use of Gaming (Adjacent) Platforms: Insights Regarding Primary and Secondary Prevention Measures” (Radicalization Awareness Network (RAN), 2021).

campus.⁴¹ Violent jihadist groups, too, have sought to develop their own games: Hezbollah has released a series of FPS games, including *Special Force I* and *Special Force II* (2003 and 2007) and *Holy Defense* (2018). As a media-savvy extremist organisation, Islamic State (IS) sought to tap into gaming by building propaganda videos based on mods, entitled *Dawn of ISIS* (2017) and *Islamic State* (2017-2021) for the FPS title *Arma 3*. The group also released content using mods for *Grand Theft Auto* in 2016.⁴² While these games receive a reasonable amount of attention and justified concern, their appeal is generally limited to sympathisers willing to seek out and actively engage with extremist content on their computers. Yet they retain utility as tools for radicalising those already sympathetic to extremist views while projecting soft power for the groups that design them.

Game Name	Date	Extremist Type	Game Name	Date	Extremist Type
Islamic Fun	1999	Islamist	ISIS Mods for Arma 3	2017-2021	Islamist
School Shooting.wad	1999	White Supremacist	Angry Goy I	2017	White Supremacist
UAC Labs	1999	White Supremacist	Tay AI	2017	Antisemitic
Under Ash	2001	Islamist	Angry Goy II	2018	White Supremacist
Ethnic Cleansing	2002	White Supremacist	Holy Defense	2018	Islamist
White Law: Sequel to ethnic cleansing	2003	White Supremacist	Jesus Strikes Back: Judgment Day (Remastered)	2020	White Supremacist / Antisemitic
Special Force	2003	Islamist	Trump 2020 Simulator	2020	White Supremacist
Deus Vult (various)	2004-2020	White Supremacist	Sharpshooter3D	2020	Neo-Nazi
Under Siege	2005	Islamist	Jesus Strikes Back 2: The Resurrection	2020	White Supremacist
ZOG's Nightmare	2006	White Supremacist	Simp Slayer Simulator 2K20	2020	White Supremacist
Special Force 2: Tale of the Truthful Pledge	2007	Islamist	Call of Russia: Furry Warfare (Putin v Furrries)	2020	White Supremacist
Muslim Massacre	2008	Islamophobic	Thot Patrol Simulator	2020	White Supremacist
Grezzo 2	2012	White Supremacist	Karen Simulator: Wagecuck v Karen	2020	White Supremacist
ISIS Mods for GTA	2014	Islamist	Nightclub Slaughter.wad	2021	White Supremacist
Moon Man	2015	White Supremacist			
Stormer Doom	2015	Antisemitic			
Fate of Islam	2016-2022	Islamophobic			

Chart four: partial index of extremist and terrorist-related games.

41 D'Anastasio, "How 'Roblox' Became a Playground for Virtual Fascists"; Kowert et al., "Breaking the Building Blocks of Hate."; Seng, "'Roblox' Und Rechtsextremismus".
 42 Ahmed Al-Rawi, "Video Games, Terrorism, and ISIS's Jihad 3.0," *Terrorism and Political Violence* 30 (4) (5 August 2016): 740-60; Reddit r/GrandTheftAuto, "ISIS Use GTA v and My Mod for Propaganda." Reddit, 2016, https://www.reddit.com/r/GrandTheftAutoV_PC/comments/4rk35o/comment/d527bix/?utm_source=reddit&utm_medium=web2x&context=3.

Gamification for Radicalisation

Gamification is, put simply, the use of elements from games in non-game environments.⁴³ Think of hotel reward points: the more nights you stay, the more points you receive and the higher your ranking. With the higher rank comes more benefits. Credit cards, airlines and countless other gamified schemes exist, including ample game-based and gamified educational tools. Gyms and fitness apps like Strava or Zombies Run! also gamify exercise to incentivise users to reach their goals. Games help improve learning, set rules and roles, and intensify engagement with content.⁴⁴

Violent extremist actors quickly adapt to new tools and utilise addictive, practical gamification approaches. Schlegel has distinguished between top-down gamification, typically deployed by extremist organisations, and bottom-up gamification tactics used by individual extremists.⁴⁵ These approaches include leader boards and award badges to rank terrorist atrocities,⁴⁶ meme-based imagery based on terrorists levelling up via their acts,⁴⁷ and apps built by IS to teach ideological indoctrination alongside Arabic to children.⁴⁸

	Top-down gamification	Bottom-up gamification
Who	Extremist organisations, recruiters, strategists	Individuals, small groups, online communities
What	Strategic use of rankings, badges, points, leader boards	Livestreaming, gamified language, virtual scoreboards, personal 'quests'
Why	Facilitate engagement with content and peers, visibility of commitment, motivate users to participate, appeal to young audience	Appeal to online community/subcultural milieu, look cool, make sense of reality via gaming content
Examples	Rankings, badges, etc in forums; apps such as Patriot Peer	Attacks in Christchurch and Halle; small-group WhatsApp radicalisation; discussions on social media – e.g. desire to "beat his score"

Chart five: top-down and bottom-up gamification reproduced from Schlegel (2021).

-
- 43 Sebastian Deterding, Dan Dixon, Rilla Khaled, and Lennart Nacke, "From Game Design Elements to Gamefulness," Proceedings of the 15th International Academic MindTrek Conference on Envisioning Future Media Environments - MindTrek '11, 2011, 9–15.
- 44 Entertainment Software Association (ESA), "Essential Facts about the Video Game Industry 2022," July 2022, <https://www.theesa.com/wp-content/uploads/2022/06/2022-Essential-Facts-About-the-Video-Game-Industry.pdf>; Robin Hunnicke, Marc Leblanc, and Robert Zubek. "MDA: A Formal Approach to Game Design and Game Research," 2004. <https://users.cs.northwestern.edu/~hunnicke/MDA.pdf>.
- 45 Linda Schlegel, "The Gamification of Violent Extremism & Lessons for P/CVE" (Radicalisation Awareness Network (RAN), 2021).
- 46 Linda Schlegel, "Connecting, Competing, and Trolling: 'User Types' in Digital Gamified Radicalization Processes," *Perspectives on Terrorism* 15 (4) (2021).
- 47 Cathrine Thorleifsson and Joey Düker, "Lone Actors in Digital Environments," Radicalisation Awareness Network (RAN), 2021, https://home-affairs.ec.europa.eu/system/files/2021-10/ran_paper_lone_actors_in_digital_environments_en.pdf.
- 48 Suraj Lakhani, "Video Gaming and (Violent) Extremism: An Exploration of the Current Landscape, Trends, and Threats," Radicalisation Awareness Network (RAN), 2022, https://home-affairs.ec.europa.eu/system/files/2022-02/EUIF%20Technical%20Meeting%20on%20Video%20Gaming%20October%202021%20RAN%20Policy%20Support%20paper_en.pdf; Lakhani et al., "The Gamification of (Violent) Extremism".

Equally insidiously, the livestreaming of terrorist attacks via online gaming-adjacent platforms has helped to gamify terror while blurring the lines between physical and virtual spaces.⁴⁹ Starting with the 2019 Christchurch attacks, far-right attackers following “cultural scripts” have emulated livestreaming tactics in subsequent attacks in Poway, Bærum, Halle and Buffalo.⁵⁰ These attacks often combine the use of helmet-camera footage with tactical weapons, armour and kit that look to emulate the visual style of FPS games. By broadcasting their attacks to audiences in real time, attackers can increase engagement with the atrocity, giving audiences a way to send support through emojis and text.⁵¹ Deploying dehumanising humour alongside video content and meme-based (or memetic) tactics, extremist attackers and viewers appear to join “play frames” where many treat the “activities that are occurring as both true and not true, serious and non-serious at the same time”.⁵² Both top-down and bottom-up gamification approaches provide effective tools for recruiting, radicalising and retaining members inside extremist groups.

Location	Date	Manifesto posted on	Livestream	Outlinking
Christchurch, New Zealand	15 Mar 2019	8chan, /pol/	Facebook	Filesharing sites by the attacker
Poway, USA	27 Apr 2019	8chan, /pol/	Facebook (attempt)	
El Paso, USA	3 Aug 2019	8chan, /pol/		
Bærum, Norway	10 Aug 2019	Endchan	Facebook (attempt)	
Halle, Germany	9 Oct 2019	Meguca	Twitch	
Hanau, Germany	19 Feb 2020	YouTube, Personal Website		Filesharing sites by supporters, Kiwifarms
Buffalo, USA	14 May 2022	Discord, Gdoc	Twitch	Filesharing sites by supporters
Bratislava, Slovakia	12 Oct 2022	Twitter (outlinked)		Filesharing sites by the attacker

Chart six: far-right attacks with gamified elements. Adapted and extended from Thorleifsson, 2021, 7.

49 *ibid.*
 50 Graham Macklin, “‘Praise the Saints’: The Cumulative Momentum of Transnational Extreme-Right Terrorism,” in *A Transnational History of Right-Wing Terrorism: Political Violence and the Far Right in Eastern and Western Europe since 1900*, ed. J Dafinger and M. Florin (London, UK: Routledge, 2022).
 51 Amarnath Amarasingam, Marc-André Argentino, and Graham Macklin, “The Buffalo Attack: The Cumulative Momentum of Far-Right Terror,” *CTC Sentinel* 15 (7) (July 2022); Lakhani and Wiedlitzka, “‘Press F to Pay Respects,’” 1–18.
 52 Cathrine Thorleifsson, “From Cyberfascism to Terrorism: On 4chan/Pol/ Culture and the Transnational Production of Memetic Violence,” *Nations and Nationalism* 28 (1) (18 November 2021), 9.

Exploiting Gaming as Pop Culture

Games now hold tremendous pop cultural appeal for millennials and younger generations who have grown up alongside games. From FPS styles in *Halo*, *Fortnite* and *Valorant* permeating online video styles and offline costumes, to sandbox pixelated trends from *Minecraft* migrating to trendy Crocs footwear, game references are everywhere. Extremists understand this and, like any good marketer, leverage pop icons to their advantage. The abovementioned livestreaming tactics draw on cultural references echoing “Let’s Play” videos where livestreaming stars play games while interacting with their audiences online.

Meanwhile, violent extremist organisations have worked video game references into their propaganda, including IS using *Grand Theft Auto V* and *Arma 3* mods to give the illusion of being able to create high-quality games.⁵³ Far-right groups, meanwhile, have produced memes and propaganda content based on “historical simulation and strategic videogames such as *Europa Universalis IV*, *Hearts of Iron IV*, and *Stellaris*”.⁵⁴ Viking aesthetics, of the sort found in numerous video games, have also been repurposed by far-right actors as memetic warfare to weaponise video game styles for propaganda purposes.⁵⁵ Using pop cultural references from gaming helps extremist actors to propagandise and recruit for their causes.

Exploiting Online Games for Communication

Violent extremist individuals and organisations also repurpose in-game chat and communication functions to recruit users and facilitate intra-group exchange. In-game chats are often less moderated than other social media platforms and unencrypted messaging apps. By approaching users while they play, racist or discriminatory humour can help recruiters quickly to identify like-minded individuals without giving away their cause.⁵⁶ These preliminary conversations often occur in toxic gaming environments where hostile humour, racism and sexism are rife.⁵⁷ By leveraging jokes, extremist actors can help to facilitate a “cognitive opening”,⁵⁸ which can then be used to create a conversion funnel to more private settings: specific servers run by the extremist group (on Discord or Telegram, for example) or by outlinking to websites owned by the organisation. Furthermore, “gaming-adjacent platforms have also been exploited by far-right ... networks to vet applicants” and share propaganda in comparatively unmoderated settings.⁵⁹ In-game chat functionalities allow rapid and easy access to a wide range of users, including younger demographics, which can help recruitment, propaganda and potentially intra-group communication efforts.

53 Isabel Garcia, “The ‘Call of Duty’ Effect: The Role of Videogames in Extremist Radicalisation” (MSc Thesis, 2022); Firas Mahmoud, “Playing with Religion: The Gamification of Jihad” (Danish Institute of International Studies (DIIS), September 27, 2022).

54 Garcia, “The ‘Call of Duty’ Effect,” 23.

55 Ashton Kingdon, “God of Race War: The Utilisation of Viking-Themed Video Games in Far-Right Propaganda,” Global Network on Extremism and Technology (GNET), 2023.

56 Anti-Defamation League (ADL), “This Is Not a Game: How Steam Harbors Extremists,” April 29, 2020; Davey, “Gamers Who Hate”.

57 Anti-Defamation League (ADL), “Caught in a Vicious Cycle: Obstacles and Opportunities for Trust and Safety Teams in the Games Industry,” www.adl.org, 2023. <https://www.adl.org/resources/report/caught-vicious-cycle-obstacles-and-opportunities-trust-and-safety-teams-games>; Anti-Defamation League, “Hate Is No Game”.

58 Simona Trip et al., “Psychological Mechanisms Involved in Radicalization and Extremism. A Rational Emotive Behavioral Conceptualization,” *Frontiers in Psychology* 10 (437) (6 March 2019).

59 Tech Against Terrorism, “State of Play: Trends in Terrorist and Violent Extremist Use of the Internet,” 2022.

Exploiting the Gaming Environment and Adjacent Platforms

As illustrated previously, the gaming environment extends far beyond only games to include online (and offline) spaces built for gamers and the many subcommunities among them. Researchers with the RAN offer that “video gaming can be an entry point where, once trust is established, there is the possibility that recruiters are able to guide people to alternative, less monitored, spaces”.⁶⁰ Specific exploits across gaming-adjacent platforms include the use of closed, pseudonymous servers on Discord to mobilise attacks, such as the fatal 2017 Unite the Right rally in Charlottesville, USA, and to create manifestos, such as the text penned by the perpetrator of the 2022 far-right attack in Buffalo, USA. Discord has a dedicated extremism policy and has stepped up enforcement efforts substantially, unlike other platforms, yet the nature of community-based chat servers continues to pose a risk for creating exclusivist extremist cells.⁶¹ As mentioned earlier, livestreaming platforms – notably Twitch, the most popular livestreaming platform, which is owned by Amazon, and Facebook Live – have also been exploited by violent extremist attackers. While platforms have become far more responsive – Twitch removed the Buffalo attack livestream within two minutes – sympathisers archive and outlink to terrorist content hosted elsewhere on the web for viewing by millions.

Additionally, the internal teams responsible for regulating harmful content, known at most platforms as ‘trust and safety’ teams, have often been cut amid budget slashes of the sort seen in early 2023. Twitch has reportedly laid off many trust and safety team members amid a company-wide reduction of staff. Similar cuts have been noted across the sector, which comes with concerns that investments in the safety and security of users may be at risk without proper resourcing. For example, Twitter has also drastically reduced its policy and trust and safety teams and has seen an alarming spike in antisemitic, violent jihadist and other forms of extremist content since the layoffs.⁶² These shifts speak to extremist actors’ active exploitation of gaming ecosystems to propagandise, recruit and mobilise and the need to prevent those attempts via proactive policy and enforcement.

Financing and Money Laundering

There are also indicative concerns of terrorism-related financing and money laundering over gaming and gaming-adjacent platforms. The scope of this phenomenon is not yet well known, with a lack of comprehensive data and research obscuring a clear view of the risks. However, there is evidence of loopholes to sell games, in-game items and other gaming products in exchange for cryptocurrency or fiat currency. For example, many games use virtual currency exchanges that often do not align with anti-money laundering (AML) standards.⁶³ Platforms are not singularly to blame: regulators worldwide do not require AML regulations for virtual worlds or gaming spaces. At the

60 Lakhani, “Video Gaming and (Violent) Extremism”.

61 Discord, “How Trust & Safety Addresses Violent Extremism on Discord,” discord.com, 2021; Tech Against Terrorism, “State of Play”.

62 Cristiano Lima, “Analysis | Antisemitic Tweets Soared on Twitter after Musk Took Over, Study Finds,” *Washington Post*, 20 March 2023; Brianna Reeves, “Twitch Starts Revealing Which of Its 400 Laid-off Employees Will Be Let Go,” *Dexerto*, 24 March 2023.

63 Shane Kelly, “Money Laundering through Virtual Worlds of Video Games: Recommendations for a New Approach to AML Regulation,” *Syracuse Law Review* 71 (1487) (2021).

same time, livestreaming services offer ways to provide streamers with gifts of in-game items in their favourite games. DLive, a platform popular with the far right, refers to itself as “the world’s primary and largest blockchain streaming channel” and allows users to easily monetise their content via an in-house cryptocurrency through its DLive Protocol.⁶⁴ The platform was used during the 6th January attack on the US Capitol and, while the public-facing site has supposedly made content regulation changes, the underlying technological structure designed to escape moderation efforts appears unchanged.

Meanwhile, the sandbox game platform *Roblox* alone took in \$2.2 billion in revenue during 2022, with between 24.5% and 29.6% of every dollar spent in-game going to individual developers who can cash out their earnings.⁶⁵ *Fortnite*, often deemed the most popular game in the world at present, earned its parent company, Epic Games, around \$5.8 billion in revenue in 2021.⁶⁶ The game features “loot boxes”, an in-game service that randomly creates in-game items in exchange for in-game currency. These loot boxes have been implicated in money laundering schemes.⁶⁷ As microtransactions of the sort seen in *Roblox*, *Fortnite* and elsewhere surge in popularity – potentially to over \$68 billion by 2023 – better regulations and efforts to keep funds from being easily converted to cryptocurrencies and laundered are clearly needed.⁶⁸ The inter-governmental Financial Action Task Force, responsible for coordinating efforts against terrorism-related financing globally, has issued warnings on the matter since 2018: those should be strengthened and heeded by member states. Until that happens or platforms voluntarily crack down on loopholes in gaming financial flows, the risk of extremist and terrorist-related financing on gaming platforms remains.

64 DLive, “DLive Protocol: Installation Guide,” 2023, <https://docs.dlive.com/docs>.

65 Roblox, “Developer Economics | Roblox Creator Documentation,” create.roblox.com, 2023; Roblox, “Roblox Reports Fourth Quarter and Full Year 2022 Financial Results,” 2023, <https://ir.roblox.com/news/news-details/2023/Roblox-Reports-Fourth-Quarter-and-Full-Year-2022-Financial-Results/default.aspx>.

66 Mansoor Iqbal, “Fortnite Usage and Revenue Statistics (2023),” *Business of Apps*, 9 January 2023.

67 Philip Conneller, “CS:GO Money Laundering Shut down by Game Publisher Valve Corp,” *Casino.org*, 6 November 2019. Kishan Mistry, “P(L)aying to Win: Loot Boxes, Microtransaction Monetization, and a Proposal for Self-Regulation in the Video Game Industry,” *Rutgers Law Review* 71 (537) (2018).

68 Shane Kelly, “Money Laundering through Virtual Worlds of Video Games: Recommendations for a New Approach to AML Regulation,” *Syracuse Law Review* 71 (1487) (2021).

4 Mitigating Extremist Harms to Gaming Spaces

Given the risks and exploits occurring in online gaming spaces, a range of efforts are underway by industry, civil society practitioners and others working to prevent and counter extremism within this ecosystem. The gaming ecosystem can itself push back against extremism by better fostering positive resilience,⁶⁹ inclusive practices and self-moderation in gaming communities while avoiding securitising the space or alienating users.

Trust and Safety Efforts

Along with the varied gaming and gaming-adjacent companies, there are also varied levels of effort exerted by these companies to prevent and counter extremism on their platforms. While some companies have put significant effort into creating or adhering to advice from bodies such as the Global Internet Forum to Counter Terrorism (GIFCT) and Tech Against Terrorism (TAT), many equally make little to no effort to moderate extremist content on their platforms. The gaming industry has historically avoided the same scrutiny applied to social media companies and has, in some ways, remained resistant to the suggestion of policy influence on its business. However, increasingly, there is attention being given to this space by governments concerning content moderation efforts and mitigation of online harms to digital services regulation.⁷⁰

In order to comply both with what legislation exists to govern their content and with their terms of service and platform engagement rules, many of the companies have what they call 'trust and safety' teams. These teams are responsible for implementing strategies, most often devised by the companies themselves and not often shared publicly, to prevent and counter the vast range of potential harms and illicit behaviours in the online gaming ecosystem. It is important to recognise that these teams are often made up of a small number of individuals compared to the vast number of users on their platforms. Also, in most cases, the individuals who comprise trust and safety teams are not researchers or experts on violent extremism and are responsible for a wide mandate of safety issues.

Where there are dedicated experts in these spaces, they often are overburdened by their workloads. Compounding this, many trust and safety teams have been cut in size at the end of 2022 and the start of 2023 amid a credit crunch for tech firms, as noted earlier.⁷¹

69 Resilience against violent extremist is a disputed term: in this report it is used with more precision by drawing on the social ecological framework of the Building Resilience Against Violent Extremism (BRAVE) model. See more here: <https://brave.resilienceresearch.org/>.

70 Center for Technology and Society, 'Caught in a Vicious Cycle: Obstacles and Opportunities for Trust and Safety Teams in the Games Industry', Anti-Defamation League, 2023, <https://www.adl.org/resources/report/caught-vicious-cycle-obstacles-and-opportunities-trust-and-safety-teams-games>.

71 Reeves, 'Twitch Starts Revealing'; Janosch Delcker, 'Twitter's Sacking of Content Moderators Raises Concerns – DW – 11/16/2022,' [dw.com](https://www.dw.com) (DW, 16 November 2022).

Similarly, content enforcement decisions based on the guidance developed by trust and safety teams are often left to a mixture of automated processes based on machine learning flagging systems and/or manual removals by moderators typically employed through third-party contractors around the world. Problematic workplace practices among moderation teams, including not least the vicarious trauma experienced by moderators, have been well documented.⁷² Therefore, it is essential for the EGRN and similar organisations like GIFCT and TAT to help to translate what knowledge has been gathered by extremism researchers into practical and easily accessible recommendations to be implemented by these teams.

Safety by Design

'Safety by Design' refers to the efforts of game designers and advisers to gaming companies to better design games or other technologies to make them resistant and resilient to misuse for illicit or harmful purposes.⁷³ There have long been networks working towards these purposes within the gaming industry globally. Historically, they have focused on other illicit behaviours and harms. However, in recent years, there has been growing awareness of the need to consider the harms of extremism as part of their efforts. Often, such as in the case of the Fair Play Alliance,⁷⁴ these networks are made up of individuals and organisations well versed in the technical design of games. They are computer scientists, graphics designers and so on, but not social scientists. Thus, they benefit from the efforts of adjacent networks, such as the EGRN, to translate research on the ideological motivations and social dynamics of radicalisation and recruitment to the online gaming environment. Equally, their understanding of game design technical opportunities and limitations can help to inform extremism researchers and policymakers on where technical content moderation and prevention are possible. However, this needs to be complemented by external efforts to prevent and counter violent extremism in these spaces.

Research efforts by members of the EGRN reveal that particular elements, such as the narrative storylines of some games such as *Far Cry V* or various Viking-themed games exploited by the far right, can be easily adaptable and exploited by extremist actors.⁷⁵ This is an example of where a design adjustment could be made by the gaming companies to avoid potential misuse of their game narrative for harm.

Positive Interventions

Just as there is potential for the online gaming ecosystem to be used for harm, there is equal and opposite potential to leverage it for societal benefit. There are many examples where the online gaming environment is used for pro-social purposes, including forming positive

72 Adam Satariano and Mike Isaac, "The Silent Partner Cleaning up Facebook for \$500 Million a Year," *The New York Times*, 31 August 2021, sec. Technology; Casey Newton, "Google and YouTube Moderators Speak out on the Work That Gave Them PTSD," *The Verge*, 16 December 2019, <https://www.theverge.com/2019/12/16/21021005/google-youtube-moderators-ptsd-accenture-violent-disturbing-content-interviews-video>.

73 "Safety by Design focuses on the ways technology companies can minimise online threats by anticipating, detecting and eliminating online harms before they occur," "Safety by Design (SbD)," World Economic Forum, n.d.

74 See: <https://fairplayalliance.org/>.

75 Kingdon, "God of Race War".

community engagements, raising money for charities, helping make learning fun and engaging, encouraging fitness and wellness and so on.

This positive use of online gaming has even been applied in the realm of P/CVE, both directly and indirectly. For example, there are a growing number of cases where police departments are using online gaming to reach and form bonds of trust with local communities or demographics where there has historically been a difficult or lacking relationship.⁷⁶ Esports, with a massive global audience, provides a prime example of where an online gaming environment can be used, much in the same way as a real-world sports environment can be, to teach principles like good sportspersonship and positive interpersonal engagement, as well as self-control and discipline. Research has shown that when esports are used as a tool, with a mentor and a mentoring aim, the online gaming environment provides an excellent platform for positive intervention and engagement.⁷⁷ While perhaps not using specifically the language of P/CVE, combating racism, sexism and other exclusivist behaviours in these spaces encourages resilience to extremist narratives and ideologies.

Gamifying Prevention Initiatives

Additionally, it is crucial to consider that, just as gamification can be used for communicating and amplifying violence, so can it be used to communicate and amplify P/CVE efforts.⁷⁸ Gamification is a tool defined by the user. Marketing companies were some of the first to develop and employ mass gamification and have been perfecting the research on how to use this approach to encourage sales for decades. As the P/CVE field looks to the future and at how to remain relevant in a space increasingly focused on online radicalisation and recruitment, it seems gamification of P/CVE efforts could be an excellent tool. Through it, practitioners can bring P/CVE interventions to the billions who spend time in the online gaming environment, making P/CVE efforts more engaging to a broader audience.

Members of the EGRN have mapped efforts where this is already taking place, extracted lessons learned,⁷⁹ and are designing and piloting their own online gaming P/CVE interventions.⁸⁰ There are many unique and exciting opportunities to explore in this space, including ways to engage gaming influencers (who often wield audiences in the thousands, if not millions) in making the online gaming space more resilient to violent extremism.

76 For example, the 'Cops vs. Kids' collaboration between the British Esports Association and the North Yorkshire Police Department. For more information see: <https://britishesports.org/news/gaming-used-as-a-successful-tool-to-build-relationships-between-police-and-youth-in-cops-vs-kids-pilot/>.

77 For more information see: C. Steinkuehler and K. Squire, "Researching the Impacts of Esports Programs for Youth," University of California Irvine, 2023, <https://connectedlearning.uci.edu/projects/researching-the-impacts-of-esports-programs-for-youth/>.

78 Lakhani et al., "The Gamification of (Violent) Extremism"; Schlegel, "Extremists' use of gaming (adjacent platforms)".

79 Linda Schlegel, "Positive Play: Can gamification support P/CVE measures?", Journal EXIT- Deutschland, 2023, 2–6; *ibid*.

80 Linda Schlegel, "Why extremists are gaming and how P/CVE can leverage the positive effects of video games to prevent radicalization," GameD, 2022, https://www.scenior.at/_files/ugd/ff9c7a_9f5f3687937b4f3384e2b0a7eac8c33f.pdf; D. Pisoiu, "Can Serious Games Make a Difference in P/CVE?," GNET, 2022, <https://gnet-research.org/2022/09/05/can-serious-games-make-a-difference-in-p-cve/>; G. P. Pech and E. A. Caspar, "Can a Video Game with a Fictional Minority Group Decrease Intergroup Biases towards Non-Fictional Minorities? A Social Neuroscience Study," International Journal of Human-Computer Interaction, 2022, <https://www.tandfonline.com/doi/abs/10.1080/10447318.2022.2121052?journalCode=hihc20>.

5 Conclusion: Looking to the Future

Considering the scale of the online gaming ecosystem and the increasing prevalence of this virtual interaction in our daily lives, it is important to look to the future and increase understanding and preparedness to grapple with potential harms and amplify positive impacts.

This report offers an overview and primer for those familiarising themselves with this space. The online gaming ecosystem is a complex and multifaceted environment. Gamers are rapidly increasing in numbers and in diversity. There is increasing evidence of the powerful identity fusion that can happen between online and offline identities, thus emphasising the importance of understanding social interaction and community formation within the gaming space. Based on this, the EGRN has been working to understand these socialisation dynamics as well as to delineate a typology of harms by which to understand the ways in which extremism can spread and the ways in which extremists can exploit this ecosystem better. Finally, this report lays out an overview of efforts that are happening within the policy and P/CVE programming spaces to try to mitigate these harms, as well as suggesting ways in which gamer communities themselves can also build positive resilience.

Recommendations

On the basis of the rapidly expanding focus on this space and the increasing relevance of networks such as the EGRN, GNET, GIFCT and TAT working at the nexus of online gaming and (violent) extremism, the following recommendations for research, policy and practice emerge:

Research

1. Understand the depth of the problem of radicalisation and extremism in gaming communities globally, looking specifically at forms of in-game hate speech and radicalisation, especially for non-English speaking audiences.
2. Analyse multiplayer games and adjacent platforms as communication channels where gamified tactics can be effectively deployed by extremist actors.
3. Increase understanding of how processes of socialisation in the online gaming environment can correlate to offline violent extremism, including expressions of misogyny and gender-based violence.
4. Develop novel research methodologies to understand and analyse new communication technologies, such as in-game content, livestreaming and audio chats.

Policy

1. Encourage knowledge cross-pollination across policy areas of P/CVE, mental health, social work and education in order to understand less resilient gamers, such as those who might lack strong communities or may be struggling with mental health challenges or isolation.
2. Provide funding for advice and guidance, such as through mental health interventions, as well as training on the online gaming ecosystem for educators, parents, youth leaders and other civil servants. This could include, for example, methods of encouraging re-direction from extremist content to valuable educational or self-improvement materials using gamified elements.
3. Track and research terrorism-related financing through gaming and gaming-adjacent platforms, such as gamified NFTs, in-game currency swaps for fiat currency and in-game item sales.
4. Formulate transnational and multi-agency approaches to enforcement of regulation and removal of terrorist-driven content in online gaming environments.

Practice

1. Improve safety-by-design platform policies and support trust and safety teams to improve content moderation and harm mitigation techniques. These efforts can be aided by liaising with the EGRN, GIFCT, TAT and other networks and organisations working to support these efforts with the necessary research and tools.
2. Facilitate positive interventions leveraging gaming for pro-social, inclusive ends. Evidence from EGRN members and other initiatives indicates positive results from – among other engagements – custom games and narratives, either for learning or to change behaviours; partnerships with gaming influencers and livestreaming stars; and mentorship and engagement programmes with esports leagues.
3. Strengthen platform terms of service and community guidelines to increase resilience of these spaces to extremism, as well as to foster inclusive community behavioral norms.
4. Implement industry gender mainstreaming strategies to encourage diversity and equality throughout the gaming ecosystem, including within gaming companies, designers, etc. to combat discrimination from the top down.



Policy Section

This policy section has been authored by Nicola Mathieson, Research Director, at the Global Network for Extremism and Technology (GNET) at the International Centre for the Study of Radicalisation (ICSR) at King's College London. This section provides policy recommendations and is produced independently from the authors of this report. Recommendations do not necessarily represent the views of the authors.

This report brings together two years of research activities by members of the Extremism and Gaming Research Network (EGRN). This report presents an extended typology of potential harms of extremist exploitation of online gaming platforms and strategies for mitigating this harm. The key findings of this report carry corresponding policy implications for technology companies and policymakers.

This policy section ensures that GNET reports provides actionable research outcomes that can inform and support technology companies and policymakers to identify and prevent extremist and terrorist exploitation of digital platforms. The policy section fulfils GIFCT's core pillar of learning to improve prevention and responses to terrorist and violent extremist attacks.

1. Technology Companies

This report has identified five core areas for action for tech companies:

- Research has long shown that playing violent games does not necessarily make people violent. However, harmful content and engagement does take place on gaming platforms that can contribute to violence. Tech companies should work to moderate better the content of gaming chat, social networking and file sharing functions to disrupt or remove extremist or hateful content from their platforms.
- This report introduced an expanded typology of potential harms of extremist exploitation of online gaming originally set out by the Radicalisation Awareness Network (RAN). This typology provides tech companies with a set of risks to mitigate against and to improve safety-by-design platform policies and product. This typology may also be leveraged to improve trust and safety teams' community and content moderation efforts.
- Tech companies can build engaging, fun games that rely on safety-by-design principles to improve gamers' experiences.
- New community-based behavioural norm change efforts can also be fostered in conjunction with gaming communities to improve self-moderation and advance more inclusive, less toxic gaming (sub)cultures.

- While gaming and gaming-adjacent platforms may be exploited by extremists, tech companies can also leverage games for positive interventions. EGRN's work demonstrates the possibility for positive interventions including custom games and narratives, behavioural change in gaming spaces and partnerships with gaming influencers and mentorship.

2. Policymakers

In addition to the report findings and their implications for technology companies, this report has also identified five core areas for action by policymakers:

- The online gaming community is not homogenous. Therefore, any policy that seeks to mitigate the risks of extremist exploitation of online gaming will need to be carefully tailored to specific platforms and communities.
- As much as online gaming presents an opportunity for exploitation, it also presents an opportunity for positive interventions. One of the core strengths and appeals of gaming is the communities inside which individuals find meaning. EGRN's work has highlighted how these communities can also help individuals bolster their resilience to radicalisation.
- Policymakers can leverage the appeal of gaming and community to design educational resources for schools, parents and children on how to stay safe while gaming.
- These educational resources can also help explain what a safe, inclusive community online looks like.
- This report identifies the use of gaming platforms for terrorism-related financing and adjacent platforms. Policies targeting terrorist financing should include gaming platforms within their remit and, most importantly, advance new policies and enforcement guidance that reflect the novel formats that financial flows take through gaming and gaming-adjacent platforms.



CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **[@GNET_research](https://twitter.com/GNET_research)**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.

© GNET