



DEFENCE AND DIPLOMACY

IN PURSUIT OF NATIONAL SECURITY

VOL. 13 NO. 4

ISSN 2347 - 3703

JULY-SEPTEMBER 2024

Special Issue: Extremism, Radicalisation and Terrorism

- Extremism in Pakistan: Assessing the Drift and Trends
Shalini Chawla
- Religious Extremism in Pakistan: An Existential Threat
Sushil Tanwar
- A Terror Haven in the (Re)making? The Spectre of Terrorism Under the Islamic Emirate of Afghanistan
Shivoam Shekhawat
- Rising Extremism and Radicalisation in the Maldives
Radhey Tambi
- Deciphering Radicalisation in India
Rahul Jain
- Harvesting Souls Online: Islamic States' Media Propaganda
Priyadarshini Baruah
- Exploiting Digital Playgrounds: How Terrorist Organisations Use Gaming for Recruitment and Radicalisation
Sounya Awasthi
- Conflict and Climate: Analysing the Environmental Fallout of Houthis' Red Sea Assault
Anadi
- Balancing Act: Combatting Islamist Radicalisation and Advancing Secular Education in Assam
Shalini Chawla and Priyadarshini Baruah
- Unmanned Aerial Systems in Counter-Terrorism Operations
Dinesh Kumar Pandey
- *Book Review*

EXPLOITING DIGITAL PLAYGROUNDS: HOW TERRORIST ORGANISATIONS USE GAMING FOR RECRUITMENT AND RADICALISATION

SOUMYA AWASTHI

INTRODUCTION

In contemporary times, the nature of extremist acts and movements has shifted from the real world to the virtual one. In this evolution, extremists are using digital spaces for recruitment, spreading propaganda, and raising funds for the functioning of organisations. In 2023, the gaming industry generated US\$ 26.14 billion in revenues through online gaming, which was 9.8 percent more than from the year 2022.

Around the world, there are roughly 1.1 billion people who identify themselves as online gamers. Most reported countries of online gaming include China, South Korea and Japan to show the

Dr **Soumya Awasthi** is a Fellow at the Centre for Security, Strategy and Technology, Observer Research Foundation, New Delhi.

largest number of participants. This global trend has received no small contribution from India to the growing gaming market.¹

The financial valuation of the Indian gaming industry remains over \$2 billion and is set to almost quadruple by 2027. Mobile gaming leads the market in India, due to both the overall affordability of mobile phones compared to other gaming consoles and because of its young population. In addition, India has also emerged as a destination country for the gaming industry. The upsurge in downloads of games such as PUBG and Roblox, further stimulating interest in both imaginary sports and eSports, would point toward a swift growth in online gaming in India.²

This paper discusses the use of video games in the recruitment and radicalisation of individuals by terrorist organisations. It highlights the dissolution of geographical limitations in digitalisation with the emphasis on problems which are global in nature.

THE SHIFT TO DIGITAL EXTREMISM

Historically, extremist groups have depended heavily on face-to-face interactions to recruit and mobilise volunteers. In-person interaction for distribution of propaganda was a typical method used to proliferate their ideologies. However, the internet has not just changed these tactics, it has revolutionised them, offering a more efficient way to reach probable recruits. Several vital developments mark the evolution of digital extremism.

Advent of Online Communities

The early internet facilitated the rise of online communities and provided a fertile ground where extremist views could be exchanged. These often started from unregulated internet forums and chat rooms. These platforms allowed for contact between people with similar beliefs, which helped them in creating a sense of belonging and validating their thinking.

-
1. Thematic Intelligence, "APAC Generates 64% of Global Mobile Gaming Revenue in 2023, reveals Global Data", Global Data, March 12, 2024, <https://www.globaldata.com/media/thematic-research/apac-generates-64-global-mobile-gaming-revenue-2023-reveals-globaldata/>. Accessed on July 16, 2024.
 2. Ibid.

- **Forums and Bulletin Boards:** Online communication gained momentum in the late 1990s and early 2000s in forums and bulletin boards. It simply provided space for users to post messages, hold deliberations and share content. Extremist groups utilised these platforms as a means to hold discussions on ideologies, propagate propaganda, and recruit new members incognito. Examples include Stormfront, which was a vital white supremacist forum and became the hub of racist and anti-Semitic content, as well as other extremist information.³
- **Chat Rooms and Inter-Relay Chat (IRC):** Along with this, chat rooms and IRC channels opened up and provided real-time communication, whereby people could have instant conversations. In that respect, the usage of chat rooms and IRC channels meant that extremists had more spontaneous and dynamic discussions. Since most of the chat rooms are temporary, tracking and monitoring by authorities was difficult, which helped propagate radical ideas with less control.⁴
- **Social Media and Evolution:** In the mid-2000s, when social media platforms such as Facebook, Twitter, and YouTube became more publicised, even wider avenues for extremists to sprout emerged. These newer opportunities provided by social media allowed extremists to reach a much greater population with a wider variety platform which made the job of recruiting and radicalising convenient for such groups.⁵ The evolution provided a digital ecosystem that supported the rapid growth of extremist groups. This shift from static forums to dynamic and interactive social media has given way to a situation where the spread of extremist ideologies is much faster and more pervasive than before.

3. Joanne Nicholson, Sean Keeling and Marigold Black, "Countering Violent Extremists Online", RAND, June 28, 2023, https://www.rand.org/pubs/research_reports/RRA2773-1.html. Accessed on July 17, 2024.

4. D. Koehler, V. Fiebig and I. Jugl, "From Gaming to Hating: Extreme-Right Ideological Indoctrination and Mobilization for Violence of Children on Online Gaming Platforms", *Political Psychology*, 44(2), 2022, <https://onlinelibrary.wiley.com/doi/abs/10.1111/pops.12855>. Accessed on July 16, 2024.

5. Mark Littler, and Benjamin Lee, *Digital Extremisms* (Palgrave Studies in Cybercrime and Cybersecurity, 2020).

DECENTRALISATION AND ANONYMITY

By definition, digital extremism is decentralised, with anonymity shielding the participants. In contrast to more traditional extremist groups, which would have some resemblance of leadership structure and members who are easily identifiable, online extremist networks are often fluid and leaderless. The implications of this decentralisation are multi-fold:

- **Leaderless Resistance:** The concept of “leaderless resistance” that is voiced by white supremacist Louis Beam suggests a hands-off approach towards extremist activities. In the model, small, independent cells, or sometimes, lone individuals, operate as free agents, guided more by shared ideologies rather than central directives. The only pressure this type of organisation places upon law enforcement is that it can identify and disrupt entire networks since there is no one central figure or organisation.⁶
- **Anonymity and Pseudonymity:** The internet provides a cloak of anonymity, furthering the ability of individuals to express extremist views without revealing their actual identity. This anonymity can allow users to take actions they may withhold from the physical world due to potential social or legal ramifications. Systems like 4chan and 8chan, with their anonymous postings,⁷ have acted as physical El Dorados of extremist rhetoric and organisation because the ideas may flow freely, while tracking users back to their identities is rather challenging.⁸
- **Fragmentation and Resilience:** Decentralised networks are robust and cannot be disrupted due to easy migration on different platforms or even creation of new ones if one online community is taken offline or is under surveillance. This creates hurdles

6. L. Smith, “Lone Wolves Connected Online: A History of Modern White Supremacy”, *The New York Times*, January 26, 2021, <https://www.nytimes.com/2021/01/26/us/louis-beam-white-supremacy-internet.html>. Accessed on July 16, 2024.

7. Teodar Mitew, “Deplatforming and Adaptation: Similarities Between Religious and Ideological Extremism”, *Georgetown Journal of International Affairs*, May 24, 2021, <https://gjia.georgetown.edu/2021/05/24/deplatforming-and-adaptation-similarities-between-religious-and-ideological-extremism/>. Accessed on July 17, 2024.

8. A. Zelenkauskaitė, P. Toivanen, J. Huhtamäki and K. Valaskivi, “Shades of Hatred Online: 4chan Duplicate Circulation Surge During Hybrid Media Events”, *First Monday*, 26(1), 2020, <https://firstmonday.org/ojs/index.php/fm/article/view/11075>. Accessed on July 16, 2024.

for the authorities to track and target online illicit activities. For example, once the major social media platforms started clamping down on extremist content, it led to several groups migrating to lesser or more permissive platforms such as Telegram, Gab, or Parler.⁹

- **The Role of Encryption:** Messaging applications such as Telegram and WhatsApp, have further allowed terrorists to communicate without fear due to the encryption feature in their services. Since both these apps provide end-to-end encryption, it is practically impossible for law enforcement agencies in particular to decode the encryption on conversations.¹⁰ This level of security has turned encrypted apps into a preferred tool in organising activities and spreading extremist propaganda.

Such inherent features within digital extremism make it difficult to counter the illegal activities of extremist groups. Therefore, it is harder to carry out traditional approaches of surveillance and infiltration when one is dealing with a situation in which suspects can often mask their identities and disperse across several platforms.

GLOBAL REACH AND ACCESSIBILITY

The global reach of digital space has transformed the way extremists are recruiting and radicalising the youth unabated. Unlike in the past, where physical proximity was often a prerequisite for radicalisation, this digital era allows real-time communication from different parts of the globe, having numerous consequences:

- **Breaking Geographical Barriers:** The virtual world has crossed all geographical boundaries. Extremist groups easily connect with people from different countries and continents and, thus, extend their influence beyond sovereign boundaries. This has provided an opportunity for extremist groups to target disgruntled and struggling for identity individuals through gaming and chat rooms. For example, *jihadist* groups originating in the Middle

9. Lei Nguyen and Oussema Othmeni, 'The Rise of Digital Extremism: How Social Media Eroded America's Political Stability', *I Volunteer International*, June 25, 2021, <https://www.ivint.org/the-rise-of-digital-extremism-how-social-media-eroded-americas-political-stability/>. Accessed on July 16, 2024.

10. Nicholson, et. al., n.3.

East have been able to recruit even people from Western countries through online propaganda and communication channels.¹¹

- **Diverse and Global Recruitment Pools:** The internet has opened up a vast and diverse pool of potential recruits. Extremists target ideological, interest, and even vulnerable targets. Online platforms allow for segmenting audiences, which consequently enables extremist groups to tailor messages for specific demographics.¹²
- **Fast Spread of Ideas:** The speed with which information, messages and news are relayed is incomparable with any other medium. Among all these, the social media platforms have been major facilitators in the fast broadcasting of extremist material. Viral videos, memes, and hashtags reach millions in seconds; this makes the spread of radical ideas widespread.
- **The Role of Diaspora and Expatriate Communities:** These communities are usually bridges between the resident country and their country of origin and, thus, easily targeted for radicalisation by different local and international actors. Far-right extremist groups in Europe, for instance, have been courting immigrant communities online, touting tenuous relations and grievances as a means of gaining possible recruits.¹³
- **Language and Translation Tools:** Many translation tools and multilingual platforms have further enabled the global spread of extremist ideologies. The availability of Artificial Intelligence (AI) tools for easy translation of extremist content into multiple languages makes it widespread. This linguistic accessibility means a radical message transmitted to different languages in no time. These tools are used strategically by extremist groups in an attempt to penetrate social discourses and further normalise their ideologies for prospective recruits and to further radicalise those already participating. For instance, the Islamic State of Syria and Iraq (ISIS) has managed to apply translations while issuing its

11. Clare Lally, "Online Extremism", *POST UK Parliament*, May 6, 2020, <https://post.parliament.uk/research-briefings/post-pn-0622/>. Accessed on July 18, 2024.

12. Jacob Ware, "The Third Generation of Online Radicalisation", Programme on Extremism, George Washington University, June 16, 2023, <https://extremism.gwu.edu/third-generation-online-radicalization>. Accessed on July 16, 2024.

13. Lally, n. 11.

propaganda in various languages, which has empowered it to permeate globally.¹⁴

ROLE OF DIGITAL GAMING SPACES

Digital gaming spaces have emerged as a key feature in the constantly evolving online extremist landscape, offering a concentrated set of vulnerable individuals for exploitation. No other online platform offers anything quite like what the interactive immersion games afford: a platform where deep influences can be forged. Features that likely make gaming platforms uniquely vulnerable to exploitation by extremist groups include diversity and reach of audience, interactivity, and immersive environments, often with inadequate moderation. These are discussed in greater detail in the sections that follow:

An Engaging and Diverse Audience

- **Global Reach and Demographic Diversity:** The most striking things about digital gaming spaces are their global reach and demographic diversity. The billions of users and the extremely varied demographics—age, gender, nationality, and socio-economic backgrounds—that gaming platforms encompass create an environment in which messaging, by extremists, can easily be tailored to particular sets of audiences. The targeting could either be toward young men in the West, for instance, since they have the tendency to engage in particular types of games, or the minority classes that may feel a sense of disfranchisement even more.¹⁵
- **Specific Targeting of Susceptible Individuals:** Second, the wide appeal found within games creates an even greater potential for

14. P. Müller, S. Harrendorf and A. Mischler, "Linguistic Radicalisation of Right-Wing and Salafi Jihadist Groups in Social Media: A Corpus-Driven Lexicometric Analysis" *European Journal on Criminal Policy and Research*, vol 28, May 12, 2022, pp. 203–244, <https://link.springer.com/article/10.1007/s10610-022-09509-7#citeas>. Accessed on July 16, 2024.

15. Galen Englund and Luxinaree Bunmathong, "Understanding the Game: Bridging Research Gaps at the Nexus of Gaming and Extremism", *Global Network on Extremism and Technology*, March 9, 2022, <https://gnet-research.org/2022/03/09/understanding-the-game-bridging-research-gaps-at-the-nexus-of-gaming-and-extremism/>. Accessed on July 16, 2024.

extremists to exploit an even greater pool of potential recruits. Such topics have been found to relate to the lives of people who show signs of weakness such as loneliness, low self-esteem, or dissatisfaction with their situation. This gaming is identified as a common activity in which such individuals can get involved and be gradually exposed to extremist ideology. It is a very effective approach since the gaming community does offer some sense of belonging and purpose that, in a way, fills some form of gap within these individual lives.¹⁶

- **Popular Games as a Means of Recruitment:** Some of the games, based on their theme, genre, or mode of play, may attract certain target groups that are very valuable to extremists for recruitment. For instance, military simulation games or first-person shooters are often appealing to those who enjoy strategy, combat, and scenarios involving historical elements. With such games, extremists could potentially reach out to players who have a pre-conditioned orientation toward particular ideologies, like nationalism or militarism, that could prepare them for the message offered during the radicalisation process.¹⁷

Immersive and Interactive Environments

- **Engagement via Gameplay:** Games are inherently interactive, and one must participate in the content and other players' engagement to take part. Such interactivity can create a deep feeling of immersion, in which individuals are completely swept into the game's world and story. Extremists can exploit such immersion by easily incorporating their messages into the gameplay. For instance, a mod or even a game level may be designed with certain specific scenes, which, in a subtle way, introduce an extremist idea, create villains from certain groups,

16. UNODC, *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System*, United Nations Office on Drugs and Crimes, 2017, https://www.unodc.org/documents/justice-and-prison-reform/Child-Victims/Handbook_on_Children_Recruited_and_Exploited_by_Terrorist_and_Violent_Extremist_Groups_the_Role_of_the_Justice_System.E.pdf. Accessed on July 16, 2024.

17. Ibid.

or may be even glorify in certain biased ways some events of the past.¹⁸

- **Narrative and Role-Playing Elements:** Many video games have a storyline; they let players role-play in different avatars and get into multiple scenarios. These can be appropriated and then utilised by extremists to craft compelling narratives that parallel or reflect their messages. For example, a video game modification could enable players to adopt the role of a character from a historical period of interest and provide a revisionist interpretation that exalts the figure's actions.¹⁹
- **Emotional and Psychological Impact:** The captivating storyline of the games can have a strong emotional and psychological impact on the gamers, so much so that an extremist message may seem normal. Engrossed in the game world, a player can be influenced on a deep and psychic level. The heated experiences and challenges those games propose can bring about intense emotions, like excitement, anger, or frustration. These emotions are exploited by extremists to channel them toward raising urgency or feelings of righteousness among players, making them easy targets for radicalisation. For example, a game that would draw a scenario of some grim future or a world torn apart by war could just as easily stir up feelings of fear and resentment for their purposes.²⁰

MECHANISMS OF RADICALISATION IN GAMING SPACES

In this case, it is not easy to talk about radicalisation, though so many mechanisms are surely important that some key elements are taken advantage of in recruitment and indoctrination by extremist groups. Such mechanisms are likely to use the unique features of digital games and the social environment they afford. The main methods are highlighted as follows:

18. Galen Englund and Jessica White, "The Online Gaming Ecosystem: Assessing Digital Socialisation, Extremism Risks and Harms Mitigation Efforts", Global Network on Extremist and Technology, May 26, 2023, <https://gnet-research.org/2023/05/26/the-online-gaming-ecosystem/>. Accessed on July 16, 2024.

19. Ibid.

20. Zixuan Jiang, "Emotional Simulation in Game AI and Its Impact on Player Experience", *International Journal of Education and Humanities*, vol. 13, no.2, 2024, <https://drpress.org/ojs/index.php/ijeh/article/view/19621>. Accessed on July 16, 2024.

Content Manipulation

Content manipulation refers to the modification or re-purposing of game elements to express extremist ideologies. Manipulation in this regard may take multiple forms, each subtly or overtly introducing players to radical ideas.

- **Modding and Customised Content:** The most popular forms of alteration of content involve changes created by users in the visual, mechanical, and narrative aspects of a game. Ideologues of extremism in content inscribe their ideologies on the face of mods. A mod can replace the standard elements of a game with symbols, characters, or scenarios that glamorise fascist regimes, manifest historical inaccuracies, or spread hate speech toward certain groups. For example, mods on games such as *Hearts of Iron IV* allow a player to alter the fate of World War II in favour of the Axis powers, tapering off some fictional neo-Nazi doctrines.²¹
- **Skins and Avatars:** Extremists make use of skins and costumes depicting controversial symbols that allow players to manage the aesthetics of their avatars. Avatars can, for instance, be dressed in the uniform of historically oppressive regimes to demonstrate normalcy in the symbols to the players subtly.²²
- **Narrative Adjustments:** Some games allow players to create their own stories or levels, which extremists can exploit to weave narratives that align with their ideologies. These narratives might include missions or storylines that glorify violent acts or historical events from a biased perspective. Such content can be particularly influential in shaping the perceptions of younger or impressionable players.²³

21. Englund and White, n.18.

22. Daniel Koehler, Irina Jugl and Verena Fiebig, "Extreme Right Radicalisation of Children Via Online Gaming Platforms", *Global Network on Extremism and Technology*, October 24, 2022, <https://gnet-research.org/2022/10/24/extreme-right-radicalisation-of-children-via-online-gaming-platforms/>. Accessed on July 16, 2024.

23. Linda Schlegel, "Playing Against Radicalisation: Why Extremists are Gaming and How P/CVE can Leverage the Positive Effects of Video Games to Prevent Radicalisation", *Global Network on Extremism and Technology*, October 19, 2022, <https://gnet-research.org/2022/10/19/playing-against-radicalisation-why-extremists-are-gaming-and-how-p-cve-can-leverage-the-positive-effects-of-video-games-to-prevent-radicalisation/>, Accessed on July 16, 2024.

- **Propaganda Games:** But besides modifying existing games, fanatics at times develop completely new games to propagate their ideas. These are rather simple in design but with a potent message, thus, acting as instantaneous vehicles for propaganda. A most vivid example is the Super Columbine Massacre RPG, which is a very controversial game wherein the player can reenact the massacre of the Columbine High School from the massacre's point of view.²⁴

Social Interactions

Social relationships in video games take an important place within the process of radicalisation. An online game allows all forms of communication: in-game chats, voice communications, forums.

- **In-Game Chats and Voice Channels:** These channels are used extensively by extremists to get in contact with potential recruits. These channels provide a real-time communication medium wherein recruiters can gauge players' reactions and gradually introduce radical ideas. The casual nature of the gaming environments makes these interactions seem less formal and threatening, lowering the defence of potential recruits.²⁵
- **Platforms of Discourse and Interaction:** Most video games have forums or discussion boards where all players playing the games can share strategies, personal experiences about the games played, and socialise. Infiltrators with extremist views take over such platforms. Normally, they start discussing neutral issues; after some time there, and when people start accepting them, they slip into more extreme topics. They also post links to websites, videos, or extremist literature that further normalises the ideology among gamers.²⁶
- **Private Groups and Servers:** Individual extremists often create private groups or servers, effectively managing access to a platform for the similarly ideologically disposed. Such platforms

24. Ibid.

25. Sam Andrews and Joshua Skoczylis, "Video Games, Extremism and Terrorism: A Literature Survey", Global Network on Extremism and Technology, November 16, 2021, <https://gnet-research.org/2021/11/16/video-games-extremism-and-terrorism-a-literature-survey/#:~:text=Likewise%2C%20research%20has%20shown%20that,messages%20are%20simply%20passively%20received>. Accessed on July 16, 2024.

26. Ibid.

often operate as echo chambers where extremist ideas are constantly reinforced without outside interference. Perhaps more important, however, such contexts also provide overt avenues of recruitment whereby current members can more intensely induct newcomers.²⁷

- **Social Recruitment:** This is the provision by which extremist groups extend the network of followers with the same interests or causes within the gaming community. In this regard, feelings of underestimation, resentment, or the need to belong to an almost tight community are the hooks they exploit before slowly introducing radical ideas and beliefs. Somehow, this tends to be more effective in war-themed games where conflict or social breakdown occurs. This is the story through which an extremist would try to propagate an ideology.²⁸

Community Building

Community formation can lie at the heart of so many varied cases of radicalisation, and belonging or the search for meaning in life may be particularly appealing to individuals who have been excluded or disenfranchised in some way.

- **Exclusionary In-groups and Cliques:** Extremists see the social environment constructed online in gaming communities like traditional social cliques. Such a relationship provides a network of exclusiveness and cohesiveness amongst members, which subsequently bolsters their notions of uniqueness and importance. Prospective recruits would often be screened beforehand to indoctrinate them into the inner group, whereby they would slowly find themselves introduced to more radical ideas.²⁹

27. Suraj Lakhani, Jessica White and Claudia Wallner, "The Gamification of (Violent) Extremism", European Commission, 2021, https://home-affairs.ec.europa.eu/system/files/2022-09/RAN%20Policy%20Support-%20gamification%20of%20violent%20extremism_en.pdf. Accessed on July 16, 2024.

28. Rachel Kowert, "Extremist Action in Digital", Global Network on Extremism and Technology, November 21, 2022, <https://gnet-research.org/2022/11/21/extremist-action-in-digital-gaming-spaces-the-role-of-identity-fusion/>. Accessed on July 16, 2024.

29. Shiraz Shaikh, "Gaining Steam: Far-Right Radicalisation on Gaming Platform", Global Network on Extremism and Technology, July 29, 2024, <https://gnet-research.org/2024/07/29/gaining-steam-far-right-radicalisation-on-gaming-platforms/>. Accessed on July 16, 2024.

- **Shared Identity and Collective Purpose:** In most of these tight-knit groups, individuals feel compelled to share an identity as well as a shared purpose. This has commonly included displaying branded event signs, engaging in communal activities, or a means of soliciting support for a cause. This, in fact, is one of the key drivers of a vigorous sense of shared identity that others in the group connect with membership to an organisation.³⁰
- **Legitimisation of Extremist Views:** Isolation within such communities can often render the internalisation of extremist ideas. In an environment wherein one constantly faces ideas of radicals without finding any opposition, in due time, such ideas start to appear rational and justified. This can be somewhat compared with living in a communal world where the extremist opinion is constantly strengthened by interlocking validations. Such practice makes reevaluation of beliefs and the exit process more cumbersome for its members.³¹
- **Activity also Encompasses Online and Offline Spaces:** Other extremist gaming communities bring their activity to a more local, community-based level, organising meetings, events, or other 'IRL' activities. Face-to-face contacts among community members solidify bonds and make the level of involvement in the community and its cause higher. Such dynamics further allow for quicker, more personalised indoctrination processes for new members.
- **Expositional Vulnerability:** Generally, extremists in gaming communities target individuals based on the vulnerabilities within that individual. This often includes those who have been socially excluded, are having a difficult time dealing with personal issues, or are going through self-identity phases in their lives. The extremists offer them something they perceive as desirable, which materialises either in the form of a friendly community or even in terms of an ideology to follow.³²

30. Ibid.

31. Lakhani, et. al., n.27.

32. Englund and White, n. 18.

In all, these are operative processes by which people in online gaming environments are subjected to radicalisation, varying from manipulative content and interactions with the co-users to community building. Coalescing these can pressurise, invite participation, or even indoctrinate users so that eventually they become susceptible to extremist conduct online, within the virtual gaming world. Surely, such a scenario calls for a multi-strategy approach, involving a mixed bag of measures, from content moderation to community management and education about the risks of online radicalisation.

RECRUITMENT AND RADICALISATION STRATEGIES

Emotional Jumpstarting and Trust Building

One of the most important strategies that extremists use in gaming contexts is “emotional jumpstarting.” The concept shows how interpersonal relationships are accelerated by sharing emotional moments of gaming. Players who go through high-pressure situations together, like competitive play or very hard missions, often come out feeling trusting of, and friends with, the rest of their team. Extremists take advantage of these quickly formed relationships to introduce and cement radical worldviews.

Research has shown close relationships to be an especially potent contribution to the vulnerability to radical ideas: for example, close family and friends may be found to be highly relevant in turning processes within a *jihadist* organisation. These forms of contact are easily established through game-playing within gaming platforms and then extended into private forums or other channels like Discord.

Functions of Narrative and Pictorial Elements

Many video games contain complicated storylines and/or visually stimulating environments. Extremist-minded individuals can leverage these elements to serve their purposes. Consider the following:

Historical Revisionism: Historical games, like *Hearts of Iron IV*, can easily romanticise and glorify fascism or other extremist ideologies. Such games, by their very design, have the ability to

subtly influence what players think or believe regarding an alternate version of history.

Symbolism and Iconography: Extremists can introduce symbols and iconography associated with their ideologies into games. This may include swastikas, imagery of Nazis, or other symbols that tend to normalise extremist views.

Propaganda Tools: Specially designed games are usually created by extremist groups as overt tools of propaganda. For example, titles like *Super Columbine Massacre RPG* and *Active Shooter* have been used in an attempt to glorify violence and propagate an extremist philosophy.³³

Secure Vetting Processes

Extremists tend to prospect for candidates for recruitment in more insular gaming communities or other, larger, and more general digital spaces. This often involves the sort of invitation into private lobbies and chat rooms extended to those who appear interested in extreme ideas. The individuals would then be gradually exposed to extremist content and introduced to increasingly radical elements of the ideology.

Such communities often give a sense of belonging and shared purpose, which may complicate the issue of leaving them. Isolation from broader contexts within society—along with the ongoing process of reinforcement of the extremist ideology within those groups—tends to speed up this process.

GUIDELINES FOR GAME DEVELOPERS

Other options among the questions of risks of extremist exploitation, which game developers and platforms might consider, include:

Content Moderation: Artificial Intelligence (AI) systems need to be hardwired into more resiliently driven content moderation, involving human moderators screening out extremist content. Where AI algorithms can recognise patterns of hate speech and radical imagery or the language of extremism, human moderators introduce contextual judgment in handling grey areas in nuanced situations. All

33. Linda Schlegel and Rachel Kowert, *Gaming and Extremism: The Radicalisation of the Digital Playground* (New York: Routledge, 2024).

this would obviously depend on updating moderation algorithms on a continuous basis to keep up with rapidly evolving extremist tactics.

Community Strategies and Enforcement: There need to be articulated community standards on hate speech, harassment, and extremist activities. Developers must make sure that guidelines are visible to all users and uniformly enforced through warnings, suspensions, and bans. All this is aided by consistent training of moderators on how to identify such behaviour and be cognisant of the rapidly changing landscape of extremism.

Counter-Extremism Organisations: Game developers should be constantly liaising with the Extremism and Gaming Research Network, Global Internet Forum on Counter-Terrorism, and Tech Against Terrorism. As a result of this collaboration, there must be the sharing of information, resources, and joint activities related to online extremism responses. The counter-extremism organisations should provide the latest tactics and response conduction updates through periodic workshops and training for game developers.

Educational Initiatives: Developers can collaborate with educators and counter-extremism experts to raise awareness about the potential risks of radicalisation among players and imbibe high digital literacy among them. In-game tutorials, public service messages, and partnerships with educational platforms would make players aware of online extremism and how to report such cases.

User Reporting Mechanisms: This can be achieved by having accessible and efficient reporting media that will help the developers address the concerns raised in due time, hence, maintaining a secure atmosphere for all gamers. Examples are in-game reporting buttons, hotlines, and options to report anonymously, where the user can do something about extremism proactively. This demands feedback on the report from the third-party developer in due time, indicating measures taken regarding the matter, thus, building confidence that motivates reporting among players.

CONCLUSION

The fact that several terrorist outfits are increasingly using these platforms for online gaming to recruit and radicalise brings into focus the changing face of extremism on the digital landscape in this

modern day. Virtual domains grow to interlink to our normal life, and where geographical contexts restrained communications and influence once upon a time, they are gradually giving way to far more rapid dissemination of extremist ideologies. This has further made the peculiar nature of this industry, targeting a wide and varied audience, ripe for abuse by extremist groups wanting to spread their dangerous messages.

The problem needs a complex and multi-level approach as regards different actors, namely the developers of the games themselves, the policy-makers, organisations that focus on counter-extremism, and, last but not the least, the greater gaming community. An active response is expected with regard to this set of decisive measures for effective countering of extremism in general, which is to guarantee not only protection from misuse but also platform security in particular, presented as safe, friendly, and secure to all participants.

The fight against radicalisation is not confined to those physical areas one would instantly think of but, in fact, is far-reaching into these immense virtual worlds where the next generation spends a great amount of its time and concentration. Because with each new and rapid stride of digitalisation and technologies being introduced and taken up, the world gets shrunk that little bit further, and better connected. It is for this reason that there should be great vigilance and encouragement to be on the front foot. One, must, indeed, encourage active counter-balances of the destabilising effects of extremist ideologies taking root and breeding within the digital arenas at the heart of young people's life experience. Therefore, only together can we really afford to dream of protecting and securing the world of international gaming from such grave and ominous threats of radicalisation and extremism.

