IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Youth Radicalisation In Age Of AI: Recruitment Pathways, Gaming Platform And Counter-Extremism Challenges

-Srishti Sinha, LL.M, University Institute of Legal Studies, Chandigarh University

-Dr. Amritpal Kaur, Professor, HOD BALL.B (Hons.), University Institute of Legal Studies, Chandigarh University

Abstract

Terrorism has changed overtime in tandem with technological advancement, evolving from hierarchical militant formations to decentralised online movements. The most recent developments in extremist recruiting and radicalisation in the twenty-first century have been artificial intelligence (AI) and online gaming environments. The combination of immersive gaming environments, algorithmic recommendation systems, and youth-driven digital subcultures has produced an ecology that is both dangerous and empowering. Extremist actor uses these platforms to create communities, disseminate false information, and prepare susceptible people, transforming routine online contacts into possible entry points for radicalisation. With the use of chatbots, deepfake technology, and AI-powered personalisation, radicals may also create appealing and focused narratives that resemble real peer interaction. The study finds key youth vulnerabilities that make young users especially vulnerable to online manipulation, such as identity problems, social estrangement, and digital immersion. The development of "serious games" for digital literacy, community policing programs like "Gaming with the Police," and gamified awareness campaigns aimed at refuting extremist narratives are among the counter-radicalization (P/CVE) approaches that are evaluated. Legal and ethical issues still exist in spite these initiatives. While proactive moderation is limited by constitutional free speech rights, surveillance powers are restricted by data privacy rules such as EU's General Data Privacy Regulation. Furthermore, disparities in international cyberlaw make it difficult to respond to online extremism in coordinated manner. The finding show that existing preventative tactics are still reactive, fragmented, and frequently ineffective in connecting with young gamers. The study suggests that a multifaceted approach is needed to mitigate AI-driven radicalisation, including cross-sector cooperation between governments, academics, and the game industry, as well as legal change and ethical AI governance. Societies cannot handle the growing relationship between AI,

youth, and extremism and guarantee that technology act as catalyst for resilience rather than radicalisation unless they adopt a comprehensive and rights-respecting strategy.

Keywords- Artificial Intelligence, Online Gaming, Youth Radicalisation, Counter- terrorism, Extremism

1. Introduction-

The phenomenon of terrorism is always evolving. It has changed throughout time in response to societal change, technical advancement, and political upheaval. In order to create fear, earlier waves of terrorism used direct acts of violence and hierarchical structures to instil fear, but as time went on, these groups got more sophisticated, decentralised, and networked in their attempts to sway public opinion and destabilise states. This shift characterised what some scholars referred to as "the new terrorism": less predictable, more deadly in aim, and more adaptable to opportunities brought up by contemporary communication and globalisation. A turning point in this evolution was brought by the introduction of the internet.[1] Extremist were no longer restricted by location and could easily and affordably project their belies across national boundaries. Digital platforms, according to research, made it possible for propaganda to reach large audiences, offered resources for education and training, and helped people locate groups that shared their problems. Online radicalisation seldom occurred alone; rather, it frequently coexisted with offline vulnerabilities including identity crises, political grievances, or social isolation. Process of radicalisation are rarely limited to the internet or physical realm, rather, they are typified by intricate and even changing relationship between the two. By the 2010s, radicals were increasingly using social media algorithms, which have a tendency to magnify sensational or emotionally charged information, making radical propaganda more visible and widespread. The recruitment and brainwashing of young people by extremist groups is changing quickly due to sociopolitical instability, ideological dispersion, and technological developments.[2] Since conventional counter-extremism tactics have found it difficult to adapt to these developments, young radicalisation is a serious issue that requires immediate international attention. The emergence of social media and the internet have changed how extremist group attract and sway youth. Group increasingly operate in digital environments, reaching potential recruits through online forums, encrypted messaging applications, and gaming platforms. The radicalisation process is sped up by the ease of extremist information, which shortens the time it takes for people to go from being passive recipients of propaganda to actively engaging in violent extremism.[3] Social media algorithms also contribute to the spread of extreme viewpoints. Echo chambers are created where extreme viewpoints are normalised because young people who interact with extremist content are often exposed to more of the same. Extremist organisations take advantages of these online spaces by creating captivating stories that appeal to disillusioned young people and give them a feeling of purpose and community. Video games have become a worldwide phenomenon that has influenced social interaction, entertainment, and culture. Millions of people are immersed in virtual worlds, making it crucial to comprehend the intricate interactions between many elements that make up game culture. Video games have evolved into enormous

[1] Bruce Hoffman, *Inside terrorism* (Columbia University Press, New York, rev.edn., 2017)
[2] Walter Laquer, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford University Press, New York, 1999)
[3] Maura Conway, "Terrorism and the internet: New Media-New Threat?" 59 *Parliamentary Affairs* 283 (2006).

online communities that link billions of people worldwide. But this quick growth also carries with it a troubling and concerning truth. Extremist organisations and terrorist organisations are increasingly exploiting gaming platforms to deceive unsuspecting people by abusing online gaming platforms and avoiding geographical restriction to reach young people all over the world. [4]Extremist group's activities involve violent video games, maybe in several ways. In order to encourage individuals, particularly young people, to engage in violent actions or other forms of violence, extremists utilise first-person video games to stimulate the experience of such action and violent games to glamorise militarised action.[5] Extremist utilise gaming gadgets and channels for safe communication in order to avoid being watched by security agencies and the police. As product of popular culture, violent video games are appropriated by extremists, who then give them right-wing or jihadi symbols. The purpose of these videos is to make extremism seem more commonplace by targeting those who are already extremists or who are inclined towards extremism. Violent videos are being used more and more frequently. Video games have developed into potent social interaction ecosystems in our increasingly digitalised society, going beyond simple amusement. Millions of young people congregate in these virtual areas every day to play and interact with each other, but they have also led to new dangers. Among them, the use of digital platforms by radicalising agents and terrorist groups to carry out recruiting and indoctrination activities stands out, especially when it comes to their growing audience of children or minors.

The advent of modern technologies and the increasing influence of social media and video games have created an environment that allows terrorist groups and radicalising agents to alter their recruitment and propaganda strategies. The COVID-19 pandemic has increased the exposure of so-called "digital natives" or "digital orphans," who grew up in a lonely environment, to cyber social media. They also have emotional vulnerabilities and lack parental supervision when utilising these online platforms. Terrorists group use these platform's anonymity and connections to spread extremist ideologies and target potential lone actors with messages meant to attract young people seeking meaning or a feeling of community.

Radicalisation– The term "radicalisation" is frequently used to define the mental process goes through when they lured down a perilous path. A person is said to be radicalised if they exhibit strong opinions in favour of terrorist groups, acts, extremist ideologies. It can be challenging to determine whether someone is getting radicalised since some of the symptoms are indicatives of other underlying problems or obstacles that are not related to radicalisation.[6]

The process through which an individual adopts extremist beliefs linked to terrorist group and terrorism. When someone is urged to adopt extreme opinion or beliefs in favour of terrorist's organisations and actions, this is known as radicalisation.

[4] Daniel F. Perez-Garcia, Luis Barragan Marquez, "Videogames, Minors and Radicalization: New Trends in Terrorist Indoctrination" 13 *Revista Internacional de Estudios sobre Terrorismo* 42 (2025).
[5] Aoife Gallagher, Ciaran O Connor, Pierre Vaux, Elise Thomas & Jacob Davey, *Gaming and Extremism: The Extreme Right on Discord* (Institute for Strategic Dialogue 2021), available at: https://www.isdglobal.org/isd-publications/gaming-and-extremism-the-extreme-right-on-discord/

[6] United Nations Office on Drugs and Crime, "Radicalisation and Violent Extremism" (July 2018).

The process by which people adopt ever more radical political, religious, or other beliefs is known as radicalisation. This may cause individual to endorse terrorism and violent extremism. Anybody may get radicalised in variety of ways, including: a person might be personally radicalised by someone or a group that actively tries to influence others to share their beliefs. By reading seeing extremist literature or content, frequently on the internet, people can also "self-radicalize" without external influence.[7]

Radicalisation on the internet is a specific problem, and it may occur through social media forums as well as online gaming sites.[8]

The term "radicalisation", which describes the slow shift towards extremism, is frequently used to describe shift in beliefs or actions. There is difference between the behavioural and cognitive aspects of radicalisation, the latter refers participation in extremist activities. The idea of radicalisation is relative and contingent on the environment in which it occurs rather than absolute.[9]

The term "radicalisation" gained a lot of attention after the terrorist act of 9/11. It is frequently used to describe the events leading up to the events leading up to the detonation of a bomb. Since the radicalisation may mean various things to different individuals and different meaning in different circumstances, a globally recognised definition has not yet been produced. This is because the idea of radicalisation is highly debated. But according to Van den Bos, radicalisation is the process of becoming more inclined to embrace and/or seek radical social changes that are in opposition to or might endanger the democratic legal system (even is so is not democratic).[10]Additionally, Hafez and Mullins pinpoint three components that may be considered crucial for a thorough comprehension of the idea: typically, radicalisation is a (1) slow "process" that involves acculturation to a (2) extreme ideology that prepares the ground for (3) violence, even if it does not make it inevitable.[11]

Online extremism- Promoting extreme, frequently violent political, social or religious beliefs online in order to radicalise people, creating online groups, and coordinate extremist actions is known as online extremism. In order to recruit and brain wash followers, it entails the production and distribution of propaganda, hate speech, and false information, which can occasionally result in offline violence and social divide. Social media and chatrooms are examples of online venues that extremist group use to attract new members and disseminate their beliefs. They produce and disseminate news articles, films, and memes in an effort to sway public opinion and advance their beliefs. Extremists can form networks, interact with like-minded people, and create common standards and expertise through online platforms.

[7]Radicalisation, *available at:* https://www.devonsafeguardingadultspartnership.org.uk/exploitation/radicalisation/ (last visited on October 15,2025).

[8]Radicalisation and the internet, *available at:* https://www.kent.police.uk/SysSiteAssets/media/downloads/kent/campaigns/radicalisation-and-the-internet-leaflet.pdf (last visited on October 15,2025).

[9] Radicalisation and Extremism, *available at*: https://www.safeguardingcambspeterborough.org.uk/children-board/professionals/exploitation/radicalisation-and-extremism/ (last visited on October 15,2025).

[10] Mitja Sardoc, *Radicalisation, violent extremism and terrorism: an interview with Quassim Cassam,* Critical Studies on Terrorism Seminar, held on (University of Warwick, 10 March 2020), *available at:* https://www.penncerl.org/wp-content/uploads/2022/09/Sardoc-2020-Radicalisation-Violent-Extremism-and-Terrorism-a.pdf (last visited on October 24, 2025).

[11] Hafez, Mohammed and Creighton Mullins, "The Radicalisation Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism" 38 *Studies in Conflict & Terrorism* 958-975 (2015).

Extremist group use the internet to manage their public image and raise funds. Videos from war zones and other visually distressing materials are used to evoke strong feelings and rally support for radical activities.[12]

AI-assisted recruitment- AI-based technologies might be used by terrorists to profile applicants and find possible recruits who fit their requirements. Potential recruits might then have their media material and communications personalised and tailored using generative AI capabilities. According to a UN study, Open AI's technologies have drawn criticism for their capacity to engage in "micro-profiling and micro-targeting, generative automatic text for recruitment purposes."[13]

According to the same study, artificial intelligence AI might be used in data mining to pinpoint those who are at risk of radicalisation, allowing terrorist messages or material to be distributed precisely. For instances, using AI-powered chatbots, they have broadcast customised messages to prospective recruits who frequently look for "violent content online or steamed films portraying alienated and angry antiheroes."[14]

Artificial intelligence (AI), virtual reality (VR), and the meta verse are being used more and more by extremist organisations to improve their recruiting tactics. AI-generated material, such as deepfake videos and automate radicalisation chatbots, allows radicals to construct very convincing propaganda customised to certain groups. Another emerging issue is the use of VR for training and hiring. Tactical planning, bomb-making, and combat scenarios may all be practiced in virtual surroundings by recruits thanks to the immersive training simulators that extremist groups can provide. The potential for VR technology to be used for extremist training and indoctrination will only grow as it becomes more widely available.[15]

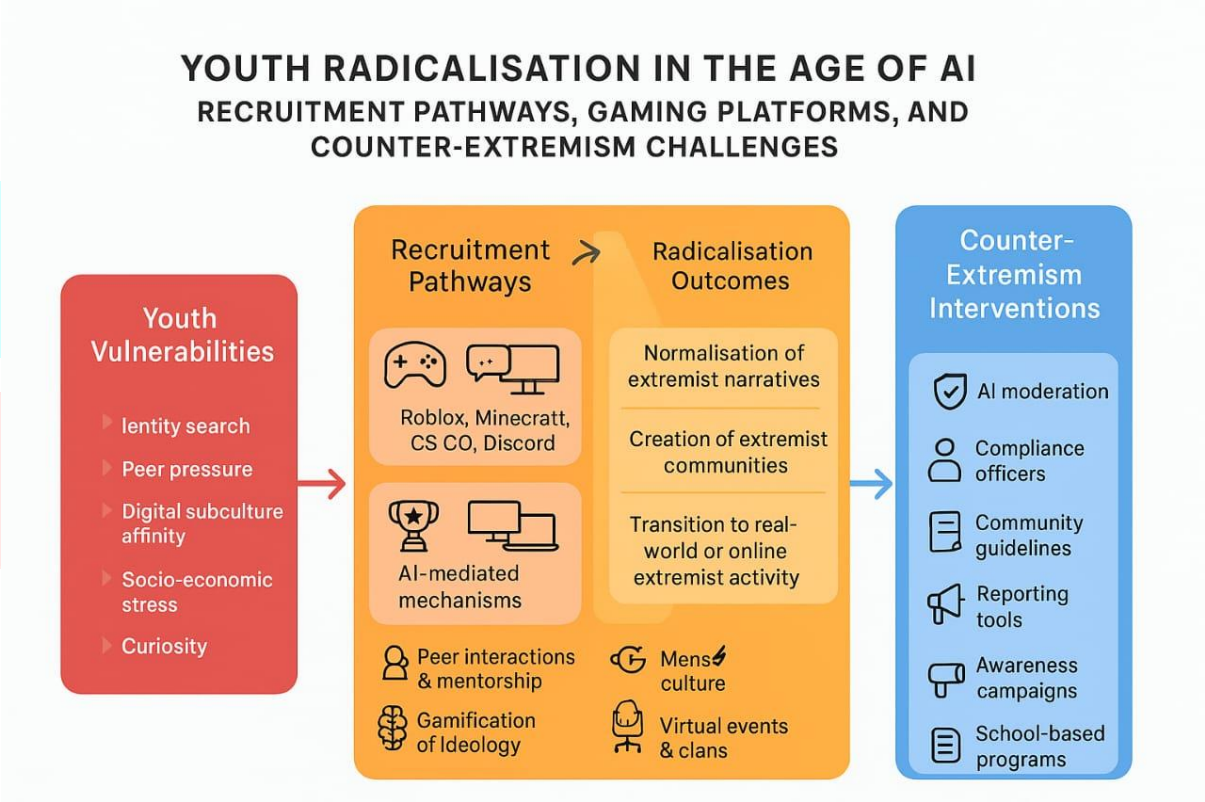
Youth radicalisation is especially severe in areas with war, poor governance and socioeconomic instability. Al-Qaeda and ISIS have long concentrated on brain washing youth in these regions, taking advantages of the lack of robust social safety nets and institutions. Generation of youth expose to radical beliefs in these unstable government might prolong violent cycles for decades to come if effective intervention is not implemented.

Extremist can use conflict areas to recruit child soldiers and subject young people to systematic radicalisation. Young people are especially vulnerable to extremist narratives that offer stability, meaning and empowerment when they experiencing economic hardship, a lack of education, and violence.

Online Radicalisation and Its New Frontiers- The digital revolution altered the radicalisation process itself, not simply how radicals disseminate their views. New methods of ideological grooming, community reinforcement, and identity- building were made possible by online settings. Online radicalisation is

[12] Parliamentary Office of Science and Technology, "Online Extremism" (POST-PN-0622, May 2020).
[13] United Nations Interregional Crime and Justice Research Institute, UN Counter- Terrorism Centre, "Algorithms and Terrorism: The malicious use of artificial intelligence for terrorist purposes" (2021).
[14] *Ibid.*
[15] Mauro Medico, *Remarks on the use of Augmented Reality and Virtual Reality in Counter- Terrorism Efforts*, webinar organised by the United Nations Office of Counter-Terrorism Efforts, Held on (New York, 8July 2021), *available at:* https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/20210708_statement_miedico_ar-vr_webinar.pdf (last visited on October 24, 2025).

frequently a mixed phenomenon, with people being formed by offline networks and grievance as well as online propaganda. It is very challenging to identify and interfere with because of this combination. With time, gaming became an unanticipated but very powerful extremist activity frontier. With billions of users globally, gaming platforms are vast platforms are vast participatory communities in addition to being places for leisure. By providing anonymity, a feeling of community, and a shared language and sense of humour, they unite young people from many backgrounds. Extremist actors take use of these characteristics by incorporating ideological statements into jokes, memes, and game-related content and establish credibility through consistent interactions in groups, guilds or private servers. Esport competitions and streaming services increase this effect by establishing venues where radical viewpoints may proliferate while masquerading as entertainment. These settings are more than just channels for communication because of their immersive and interactive features; they are social ecosystem where concepts may gradually become more accepted.[16]



2. The Shifting Landscape of Radicalisation-

2.1 From Physical to Digital- The prevailing technology of their day have always been reflected in radicalisation.[17] To spread their ideas, radicals in the 20th century used video recording, cassettes, and brochures. [18]Early media competence was displayed by organisations like Hezbollah and al-Qaeda, which used satellite television and VHS recordings to establish a worldwide presence. [19]During this time, terrorism also got more dispersed, with organisations becoming more adaptable and eager to take use of

[16] Rachel Kowert, Alexi Martel, William B. Swann, "Not just a game: Identity fusion and extremism in gaming cultures" 7 *Frontiers* (2022).
[17] United States Institute of Peace, "Special Report, How Modern Terrorism uses the Internet" (March 2004).
[18] RAND Cooperation, "Radicalization in the Digital era: The Use of the Internet in 15 Cases of Terrorism and Extremism" (2013).
[19] Centre for Strategic and International Studies, "Understanding Hamas's and Hezbollah's Uses of Information Technology" (July,2023).

new technology. Extremist communication was drastically changed by the internet. Three important benefits of the internet world were interaction, global reach, and anonymity. People might now radicalise themselves from home without of needing to physically enter radical location.[20] The evolution of extremist communication from static websites in the 1990s to interactive forums and, ultimately, the dark web underscores the adaptability and durability of extremist actors.[21]

2.2 The Era of social media- The advent of social media ushered in a new age of radicalism.[22] Extremists were able to swiftly and affordably reach millions of people thanks to websites like Facebook, YouTube, and Twitter. Sensational material was rewarded by algorithms, which frequently boosted extremist messaging. [23]Particularly with younger audiences, humour, memes, and vital material become effective means of normalising extremist beliefs.[24] As mainstream outlets become more moderate, radical once again adjusted. A lot of them switched to private servers or encrypted chat applications so they could keep communities intact with less chance of interruption.[25] More and more, the process of radicalisation became a hybrid, influenced by both online and offline concerns. Distinguishing online radicalisation from more general societal dynamics is challenging due to this merging of effects.[26]

2.3 The New Frontier of Online Gaming- Online gaming has become a new recruiting frontier in recent years. [27]Extremist actors find gaming platforms appealing since they are home to sizable youth populations.[28] These areas provide anonymity, shared humour, and immersive experiences while fusing entertainment with social interaction.[29] Extremists take use of these characteristics by incorporating ideological indications into user- generated material, memes, and in game discussions. Through private servers, guilds, and clans, they gradually gain trust while frequently passing off recruiting as friendship or mentoring.[30] This effect is further expanded by streaming services and esport groups, which provide radicals an indirect audience through entertainment culture.[31]

[20] National Institute of Justice," The Role of the Internet and Social Media on Radicalisation: What Research Sponsored by the National Institute of Justice Tells us" (April 2024).
[21] Jens F Binder, Jonathan Kenyon, "Terrorism and the internet: How dangerous is online radicalisation?" *Frontiers in Psychology* (2022).
[22] Extremism increasingly spread via mainstream apps and sites, government research finds, *available at:* https://www.publictechnology.net/2022/12/16/defence-and-security/extremism-increasingly-spread-mainstream-apps-and-sites-government-research-finds/ (last visited on October 23, 2025).
[23] *Ibid.*
[24] Rafiq Ahmad, Sumaira Saleem, "Ethical and Legal Challenges of Artificial Intelligence: Implications for Human Right "2 *Journal of Law, Society, and Policy Review* (2025).
[25] Nava Nur Aniyah, "Online extremism: the advent of encrypted private chat groups" in Edwin Jurriens, Ross Tapsell (eds.), *Connectivity and Divergence* 5-6 (ISEAS- Yusof Ishak Institute, 2017).
[26] How Memes and Internet Irony Are Hijacked for Radicalization, *available at:* https://www.asisonline.org/security-management-magazine/articles/2021/05/how-memes-and-internet-irony-are-hijacked-for-radicalization/ (last visited on October 23,2025).
[27] Extremism in Gaming Spaces: Policy for Prevention and Moderation, *available at:* https://www.rusi.org/explore-our-research/publications/policy-briefs/extremism-gaming-spaces-policy-prevention-and-moderation (last visited on October 23,2025).
[28] *Ibid.*
[29] *Ibid.*
[30] How Extremists exploit online gaming platforms to recruit young players, *available at:* https://reinouttebrake.com/2025/03/08/how-extremists-exploit-online-gaming-platforms-to-recruit-young-players/ (last visited on October 23,2025).
[31] How the Far right exploded on Steam and Discord, *available at:* https://www.wired.com/story/far-right-took-over-steam-discord/ (last visited on October 23,2025).

2.4 The Rise of AI in Radicalisation- These dangers have increased due to artificial intelligence.[32] Users are directed towards more radical content via recommendation systems, which steer them away from mainstream interests. [33]The coded language and cultural allusions prevalent in extreme subcultures are difficult for automated moderation of identify.[34] Generative AI has now made it feasible to produce convincing propaganda, including tailored recruiting messages, synthetic avatars, and phoney movies. However, AI also offers preventative options.[35] It may be used to flag hazardous information, identify extreme trends, and create instructional materials. But AI's dual function as a preventative measure and an extremist weapon makes governing more difficulties of governance in the digital era.[36]

3. Recruitment Pathways in the Age of AI and Gaming

3.1 Gaming sites as Centres for Hiring- Because gaming platforms combine three potent features- community building, anonymity, and lax moderation- they have become breeding grounds for the recruitment of extremists.[37] In contrast to conventional social networking sites, these places let users to establish pseudonyms and avatars, which makes it more challenging to identify actual users.[38] Because of this anonymity, people can talk freely and frequently without worrying about being held accountable. The feeling of belonging is just as important. Guilds, clans and teams are essential to many multiplayer games and help players form strong ties with one another. By progressively normalising radical views in welcoming, trusting surroundings, extremists' recruiters take advantage of these connections. [39]Furthermore, compared to mainstream social media, gaming environments may have laxer moderation requirements. There are blind spots where extremist messages may spread unchecked because companies frequently place a higher priority on user engagement and gaming quality than policing extremist activities.[40] Discord servers used by far-right groups are notable example. With its secret servers that allowed radical propaganda, memes, and manifestos to be exchanged covertly, Discord was once created for team communication in online games became a focal point for extremist communities.[41] This is similar to how extremists used forums in the past, but it's deeper and engaging.

3.2 Social Engineering and In-Game Communication- voice chat, private messaging, and in game communication may all be used as recruiting channels since gaming is more than just entertainment. [42]Under the pretence of having similar gaming interests, recruiters frequently employ social engineering

---

[32] Artificial Intelligence and Radicalism: Risks and Opportunities, *available at:* https://extremism.gwu.edu/artificial-intelligence-and-radicalism-risks-and-opportunities (last visited on October 23,2025).
[33] Joe Whittaker, Sean Looney, "Recommender systems and the amplification of extremist content" 10 *Internet Policy Review* (2021).
[34] AI at the centre: violent extremist exploitation in Pirkkala, *available at:* https://gnet-research.org/2025/07/14/ai-at-the-centre-violent-extremist-exploitation-in-pirkkala/ (last visited on October 23, 2025).
[35] Warisha Rashid, "Using Artificial Intelligence to Combat Extremism" 5 *Pakistan Journal of Terrorism Research (2023).*
[36] *Supra 28.*
[37] Study finds radicals nutjobs targeting gamers via Discord, Twitch, Steam, *available at:* https://www.theregister.com/2025/08/04/gaming_platforms_radical_recruitment/ (last visited on October 23,2025).
[38] *Ibid.*
[39] *Ibid.*
[40] *Ibid.*
[41] Case study: Alt-platform Discord, a haven for Islamist and Catholic extremist activity, *available at:* https://www.isdglobal.org/digital_dispatches/case-study-alt-platform-discord-havens-islamist-and-catholic-extremist-activity/ (last visited on October 23,2025).
[42] National Counterterrorism Centre (United States), "Terrorist Exploitation of Online Gaming Platforms" (October 2023).

techniques, making friends with younger gamers and gradually introducing extreme themes.[43] Private servers have been identified as potentially extremist areas, particularly in games like Roblox, Counter-Strike, and Minecraft. Games become virtual training and indoctrination tools when gamers construct propaganda-filled maps, create bespoke surroundings or even mimic assaults within these restricted communities.[44] For instances, extreme players have been observed simulating mass shootings on Roblox, obfuscating the distinction between violent video games and the real world. Recruiters also take use of audio chat capabilities. Voice chat offers ephemeral communication that leaves minimal trace, making it more difficult for law enforcement to monitor than written information, which may be detected or reported.[45] Extremist group sympathisers have been known to infiltrate chatrooms during esport events to gauge participant's openness before inviting them to off-platform forums.[46]

3.3 AI- Powered Grooming and Personalisation- The incorporation of AI-driven personalisation is what makes gaming recruitment particularly worrisome these days. Recommendation algorithms, which are employed by streaming services and gaming platforms, can identify young people who are at risk based on their online conduct, interests, and playtime. [47]Although these technologies were not created with extremism in mind, they may be used to lead users into more extremist environments. Teenagers who often play first-person shooters with military themes, for instance, could be more likely to be recommended radical memes or extremist war videos on related sites.[48] As a result, AI can serve as a grooming accelerator, providing customised extremist material that appeals to the player's gaming persona. In order to start and continue interactions with possible recruits, radicals are also experimenting with chatbots that are created by artificial intelligence.[49] In a manner, these bots, which have been educated on extreme messaging, can offer 24/7 participation and normalise radical debate. According to certain claims, deepfake avatars are being used in gaming environments to disguise extremist recruiters as friends or even influential members of the gaming community.[50]

3.4 Extremism's Gamification- Gamification of radical ideology is one of the most pernicious tactics. Gaming platforms are being used more and more by extremists and terrorist groups to attract new members and spread their ideology. Changing in game elements to represent extreme beliefs, such as settings, stories, or character skins, is a popular strategy.[51] White nationalist symbols and far-right extremist-modified video games such as Counter-Strike: Global Offensive, Islamic State have also created bespoke

[43] Libby Brooks, "Far-right extremists using games platforms to radicalise teenagers, report warns", *The Guardian*, 31 July 2025, *available at:* https://www.theguardian.com/politics/2025/jul/31/far-right-extremists-games-platforms-radicalise-teenagers-report (last visited on October 23,2025).
[44] Playing with Hate: How Far-Right Extremists Use Minecraft to Gamify Radicalisation, *available at:* https://gnet-research.org/2025/07/02/playing-with-hate-how-far-right-extremists-use-minecraft-to-gamify-radicalisation/ *(*last visited on October 23.2025).
[45] Jamie Seidel, "Inside the dark world of 'killer gaming culture'" *news.com.au*, 20 September 2025, *available at:* https://www.news.com.au/technology/online/inside-the-dark-world-of-killer-gaming-culture/news-story/ (last visited on October 23,2025).
[46] *Ibid.*
[47] *Supra 29.*
[48] *Supra 29.*
[49] *Supra 28.*
[50] International Centre for Counter- Terrorism, "The Weaponisation of Deepfakes: Digital Deception by the Far-Right" (December, 2023).
[51] *Supra 38.*

adaptation (modification) for games like Call of Duty that have political or nationalistic connotations, normalising extremist ideology via repeated exposure.[52] These immersive games work well because they keep players absorbed for extended periods of time, which gives radicals the opportunity to create groups that gradually brainwash users. [53]Furthermore, by immersing players in altered environments that support specific beliefs, virtual reality (VR), which enable real-time and customised interactions, provide extremists a window to attract young susceptible players.[54] Video game concepts like quests, leaderboard, points and achievements are used by extremist groups to make radicalisation fun and lucrative.[55] Instead of being portrayed as a moral or political responsibility, the story of "joining the cause" is one of the exciting challenges, like to advancing a video game.[56] Extremist recruiters have been seen in esport groups presenting their beliefs as a fight against outsiders, frequently members of racial or religious minorities. Players are rewarded for producing extreme material or disseminating propaganda through memes and in-game competitions. As an illustration, neo-Nazi organisations have disseminated "kill count" memes, which elevate actual violence by portraying it as a high gaming score.[57]

4. Youth Risks and Concerns-

Young people are frequently noted as one of the most vulnerable groups in both offline and online radicalisation processes. The strategic value of hiring young people has long been acknowledged by extremist organisations, since young people are more flexible, used to using technology, and receptive to new identities. These risks are heightened in the context of Ai-driven surrounding and online gaming as these areas are an integral part of young people's everyday social and cultural life.[58]

4.1 Psychological and Developmental Risk Factors- Young adulthood and adolescence are crucial times for identity development when people struggle with autonomy, recognition, and belonging. Because of this, young people are particularly receptive to stories that provide direction and clarity. Extremist recruiters take advantage of this by promising empowerment and bravery, as well as straightforward worldview that is split between good and evil. A psychological hook is added by gaming, whose immersive storylines and integrated incentive systems are modelled after the organisational framework of radical movements. Violent extremist organisation purposefully uses gaming- like elements, such as quests, battles, and achievements, to stylise their messaging in order to appeal to young people's psyche. In order to lessen psychological resistance to extreme conduct, extremist recruiters normalise violence as "play."[59]

[52] Institute for Strategic Dialogue, "Gaming and Extremism: The Extreme Right on Steam" (2021).
[53] *Supra 38.*
[54] Radicalisation Awareness Network (RAN), "The Gamification of Violent Extremism & Lessons for P/CVE" (European Commission, 2021).
[55] *Ibid.*
[56] *Ibid.*
[57] Ben Makuch, "A US neo- Nazi fight club is using Charlie Kirk's killing to recruit new members" *The Guardian*, 19 September 2025, *available at:* https://www.theguardian.com/us-news/2025/sep/19/active-clubs-charlie-kirk-killing-new-members (last visited on October 24,2025).
[58] Youth Radicalisation: A new frontier in Terrorism and security, *available at:* https://www.visionofhumanity.org/youth-radicalisation-a-new-frontier-in-terrorism-and-security/ (last visited on October 23,2025).
[59] Online Radicalisation, *available at:* https://www.aacap.org/AACAP/Families_and_Youth/Facts_for_Families/FFF-Guide/Online_Radicalization-143 (last visited on October 23,2025).

4.2 Vulnerabilities of Social and Peer Groups- One of the most potent factors influencing young people's conduct is peer pressure. In gaming settings, where loyalty and collaboration are essential, recruiters use peer dynamics as a luring tool. This vulnerability exacerbates in the esports environment. Extremist organisations have purposefully penetrated streaming services and esport chat rooms, disseminating vile messages that pass for comedy. Once accepted by peers, this humour can lead to more extreme material. Additionally, recruiters sneak into Discord channels and gaming clans, progressively reorienting conversations from gaming tactics to more general social and political concerns. Young people's defences are weakened by their peers' credibility, which increases the persuasiveness of radical narratives. The bar for accepting propaganda is much reduced once peer group start using radical lingo or humour.[60]

4.3 Political and Socioeconomic Risks- It is unusual for radicalisation to happen in a vacuum. Youth from underprivileged groups are disproportionately targeted, regardless of their economic status, religion, or nationality. Young individuals who are unemployed or lack possibilities are drawn to online spaces where extreme recruiters provide cash incentives, a sense of connection, and purpose. Radicalisation frequently thrives on grievances pertaining to discrimination or exclusion from political life. Anyone with internet connection may access gaming areas, which provide as a platform for manipulating and expressing these grievances. Some organisations portray joining violent movements as a way to get out of poverty and marginalisation, while others use minorities as scapegoats to appeal to young people who are struggling financially.

4.4 Vulnerabilities in Culture and Subculture- Additionally, digital subcultures have a significant impact on youth.[61] In gaming communities, violence, rivalry, and martial aesthetics are frequently valued.[62] Extremists' propaganda blends ideological substance with preexisting subcultural norms to mix in with these settings. Memes glorify violence as humour, and extremist ideologies are occasionally reframed as "team rivalries" in esports. [63]These settings normalise narratives of exclusion, making extremist language seem innocuous until it becomes more extreme.[64]

4.5 AI and Algorithmic Vulnerability Amplification- All of these weaknesses are exacerbated by AI.[65] Young people may be trapped in extreme echo chambers by recommendation algorithms that are intended to increase interaction.[66] Algorithms frequently recommended increasingly extreme information to young people when they engage with military or conspiratorial content. [67]Additional risks are introduced by generative AI. Chatbots that have been trained on extremist content can provide lonely young people

[60] *Supra 39*.
[61] Radicalisation Awareness Network, "Extremists' use of gaming (adjacent) platforms insights regarding primary and secondary prevention measures" (European Commission, 2022).
[62] United Nations Office of Counter-Terrorism, "Examining the Intersection between gaming and violent extremism" (2022).
[63] *Supra 39*.
[64] *Supra 57*.
[65] Gaurav Goswami, "AI Echo Chambers: How Algorithms Shape Reality, Influence democracy, and fuel misinformation" *TechRxiv* (2025).
[66] *Ibid.*
[67] *Ibid.*

ongoing company by pretending to be interested and sympathetic while quietly radicalising them. [68]AI-generated influencers and deep fake avatars can infiltrate gaming environments by posing as peers and disseminating extremist content.

4.6 Intersectionality and Cumulative Risk- Vulnerabilities among youth are rarely isolated. Rather, they work in together to make an adolescent far more vulnerable if they are exposed to extreme subcultures is at significantly greater risk because of the cumulative effects of these factors.[69] Understanding how risk variables interact is crucial, particularly as Ai-driven targeting increases their influence.[70]

5. Challenges of Counter- Extremism

In the era of AI-driven technology and gaming platforms, combating extremist indoctrination poses number of difficult obstacles.[71] Despite efforts by governments, civil society, and tech businesses to adjust, the rate of technological advancement frequently surpasses the capabilities of regulation and prevention.[72] The AI arms race, the difficulties of keeping an eye on hidden online areas, the conflict between free and hate speech laws, and the intricate duties of game companies are the four main issues that stand out.[73]

5.1 The Arms Race in AI- In the battle against extremism, artificial intelligence has evolved into both weapon and a defence.[74] Extremist organisation is using AI technologies to produce propaganda, build bots for widespread distribution, and take use of algorithms for targeted personalisation.[75] However, companies and governments are creating AI-powered moderation tools to identify and eliminate extreme material.[76] The result of this is what many observers refer to as a "AI arms race" between regulators and recruiters. However, AI moderation methods have significant drawbacks.[77] Automated programs frequently have trouble understanding subtleties of context, such the difference between extreme propaganda, satire, and genuine opposition. While false negatives let dangerous information spread, false positives can lead to excessive restriction.[78] Extremist organisations purposefully take advantage of these flaws by employing symbols, memes and coded language that avoid discovery. Additionally, the availability of radical content has significantly increased due to generative AI. By producing propaganda on a large scale, tools like text to image converters and deepfakes can lessen the need for human agents. [79]The use of generative AI by extremists for recruiting avatars, training materials, and false news presents

[68] How extremists are manipulating AI chatbots, *available at:* https://www.lowyinstitute.org/the-interpreter/how-extremists-are-manipulating-ai-chatbots (last visited on October 23, 2025).
[69] *Supra 58.*
[70] *Supra 61.*
[71] Exploitation of Generative AI by Terrorist Groups*, available at:* https://icct.nl/publication/exploitation-generative-ai-terrorist-groups (last visited on October 23, 2025).
[72] The Digital Services Act, *available at:* https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act (last visited on October 23, 2025).
[73] Royal United Services Institute, "Extremism in Gaming Spaces: Policy for Prevention and Moderation" (February, 2025).
[74] *Supra 67.*
[75] Gabriel Weimann, Alexander T. Pack, Rachel Sulciner, Joelle Scheinin, Gal Rapaport, David Diaz, "Generating Terror: The Risks of Generative AI Exploitation" 17 *CTC Sentinel* (2024).
[76] United Nations Office of Counter-Terrorism/ United Nations Counter- Terrorism Centre & United Nations Interregional Crime and Justice Research Institute, "Countering Terrorism Online with Artificial Intelligence: An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia" (2021).
[77] *Supra 67.*
[78] *Supra 69.*
[79] *Supra 67.*

a near- existential threat to the framework already in place to combat radicalisation, according to certain authorities 'warnings.[80]

AI tools have been used by extremists to automate recruiting, create propaganda, and circumvent moderation. Platforms are rushing to implement AI- based detection, but regulatory limitations on data access and surveillance are slowing down the process. The General Data Protection Regulation (GDPR) of the European Union prohibits platforms from keeping or analysing personal data for purposes other than those that have been stated. Although anonymity is preserved, this stops extensive gaming platform surveillance for extremist signals. In an effort to strike a compromise, the Digital Service Act (DSA, 2022) mandates that "very large online platforms" evaluate systematic hazards. Including extremist material, nevertheless, implementation varies.[81]

The First Amendment severely restricts state control over internet communities in the US. In Brandenburg v. Ohio, the Supreme Court created the "imminent lawless action" rule, which states that punishing extreme propaganda is illegal unless it clearly calls immediate violence. Because of this high hurdle, radical narratives can lawfully spread unless they are explicitly related to illegal conduct.[82]

India has taken the opposite course. Discord and WhatsApp are directly impacted by the Information Technology Rules 2021, which require the "first originator" of conversations on encrypted platforms to be traced. But in Shreya Singhal v. Union of India, the Supreme Court showed judicial opposition to overbroad censorship by invalidating Section 66 A of the IT Act for being ambiguous and stifling online speech.[83]

These legal conflicts highlight the reasons why the AI arms race is still skewed in favour of extremists while regulators are bound by principles of free speech and privacy, radicals take advantage of legal loopholes and technological advancement.

5.2 The dark side of internet- The movement of extremist activity into unregulated and secret areas is second significant obstacle. [84]Extremist organisations are turning to secret server, encrypted channels, and communication tools designed specifically for gaming, while mainstream social media sites are coming under more scrutiny. [85]Platforms for gaming let players to set up private, password-protected servers that act as recruiting centres. Because moderating is decentralised and frequently entrusted to the server owners themselves, these areas are notoriously hard to monitor. By introducing radical conversations into what appear to be harmless gaming communities, extremist organisations take advantage of these blind spots. Communication's transient nature makes the issue worse. A large portion of voice chat or in game

[80] *Supra 67.*
[81] *Supra 68.*
[82] 395, U.S. 444 (1969).
[83] Shreya Singhal v. Union of India, *available at:* https://globalfreedomofexpression.columbia.edu/cases/shreya-singhal-v-union-of-india/ (last visited on October 24, 2025).
[84] *Supra 69.*
[85] *Supra 69.*

correspondence is undetectable, making law enforcement surveillance all but impossible, in contrast to social media post that may be sorted. The chat has already vanished by the time investigators are notified.[86]

Extremist go from popular games to modified environments with less oversight, secret severs, and encrypted communications. The laws that govern these areas differ greatly.

There are blind spots in Europe because the DSA places requirements on major platforms like Twitch and Discord but not so smaller, specialised servers.

Platforms are protected from responsibility for user-generated material in the US by Section 230 of the Communications Decency Act. because of this, businesses are reluctant to take strong action to control radical usage of private servers.[87]

If platforms in India don't take down illegal content after being notified, they risk losing "intermediary immunity" under Section 79 of the IT Act. However, enforcement may overshoot due to the Unlawful Activities (Prevention) Act's (UAPA) broad definition of "unlawful".[88]

A "jurisdiction shopping" issue is brought on by the absence of consistent international regulations; extremist just relocate their activities to least controlled online areas.

5.3 Free Expression v. Hate Speech- The dilemma moderation efforts for extremist content are complicated by the moral and legal quandary of free speech. Democracies exercise caution when giving companies and governments broad censoring authority.[89] Moderation of information is necessary for safety, but removing too much might undermine democratic norms and even feed persecution tales from extremists.[90] Extremists are good at taking advantage of this problem. By framing their messages as free speech or portraying themselves as censorship victims, they gain sympathy from larger online groups. [91]Because different countries have quite different legal frameworks for controlling online extremism, it can be challenging to coordinate efficient actions. The development of hate speech regulations sometimes lags behind that of technology. For instance, coded language and extremist memes that circulate in esport groups may not fit the conventional criteria of incitement, yet nevertheless foster radicalisation. This puts regulators in a never-ending game of catch-up.[92]

A major legal conundrum is how to strike a balance between counter-extremism and free speech.

The US is notable for its robust safeguards. In 2010 case of Holder v. Humanitarian Law Project, the Supreme Court maintained prohibitions on giving terrorist organisations "material support," including

[86] *Supra 69.*
[87] The Communication Decency Act, 1996, s.230.
[88] The Information Technology Act, 2000 (Act 21 of 2000), s.79.
[89] Kenneth Roth, "How do we defend free speech-without falling prey to extremism?" *The Guardian,* 21 February, 2025, *available at*: https://www.theguardian.com/commentisfree/2025/feb/21/jd-vance-far-right-censorship-free-speech (last visited on October 24,2025).
[90] *Ibid.*
[91] *Ibid.*
[92] *Ibid.*

verbal support.[93] However, the court limited such limits in Packingham v. North Carlima, ruling that access to social media is a basic right.[94]

Court in Europe take a more interventionist approach. In the 2019 CJEU decision in Glawishnig- Piesczek v. Facebook, global removal responsibilities were affirmed, holding platforms accountable for extremist content around the globe. The 2020 Avia Law in France sought to require the removal of hate content within 24 hrs, however it was declared unlawful due to excessive scope.

Free speech rights under the Indian Constitution were upheld by Shreya Singhal, yet those accused of spreading extremist information online are still being prosecuted under the UAPA. The disparate methods highlight the challenge of creating consistent anti-extremism legislation.[95]

5.4 The function and duty of Gaming Companies- The role that gaming businesses play is also an obstacle. Although social media businesses have been under pressure to implement stricter content control, gaming companies have just lately been subject to scrutiny. Many contend that rather than serving as speech controls, their main function is to entertain. There are structural issues facing the sector. Scaling up the moderation process is expensive and technically complex. Millions of people play games every day, which creates lot of communication, most of it brief and situation-specific. Since younger gamer perceive censorship as obtrusive, excessive modernisation runs the danger of alienating users. Furthermore, there is currently no precise legal structure outlining gambling platform's obligation.[96]

A significant obstacle in the fight against extremism on gaming platforms is amount of information produced and disseminated in these online spaces. Developers find it challenging to keep on all activity in real time since games like Roblox and Grand Theft Auto V provide expansive sandbox settings where players may alter material at will. To identify extremist content, artificial intelligence-based detection techniques are continuously being developed. However, the quick development of extreme strategies and restrictions on data access and privacy limit these tools.[97] Furthermore, combating extremism frequently requires more specialised resources from gaming firms, some of which prioritise in game revenue over public safety. Knowing that real-time moderation is sometimes underfunded or inefficient in identifying covert radicalisation efforts, extremist groups take advantage of this weakness. Counter- radicalisation tactics have found it difficult to adapt to the changing landscape of youth extremism, despite heightened awareness. While educational system lacks the resources to recognise and respond to early indicators of radicalisation, law enforcement organisations frequently encounter ethical and legal challenges when monitoring children. Furthermore, rather than being preventive, counter-extremism strategies are frequently reactive. Instead of investing in long-term methods to prevent radicalisation from developing

[93] 561 U.S. 1 (2010).
[94] 582 U.S. 98 (2017).
[95] Constitutionality of India's Unlawful Activities (Prevention) Amendment Bill, 2019: India's McCarthyism Moment, *available at:* https://ohrh.law.ox.ac.uk/constitutionality-of-indias-unlawful-activities-prevention-amendment-bill-2019-indias-mccarthyism-moment/ (last visited on October 24,2025).
[96] The Importance of Content Moderation in Gaming, *available at:* https://chekkee.com/the-importance-of-content-moderation-in-gaming/ (last visited on October 24,2025).
[97] Nurturing the Wellbeing of Content Moderators in Gaming, *available at:* https://www.zevohealth.com/blog/nurturing-the-wellbeing-of-content-moderators-in-gaming/ (last visited on October 24,2025).

in the first place, governments and security services often concentrate on destroying terrorist networks after it has already occurred.[98]

Despite being on the front lines of preventing extremism, gaming companies are still not given enough legal protection or obligations.

In the EU, stringent liability regulations are enforced by the DSA and NetzDG (2017, Germany). Businesses risk severe fines if they don't delete extremist information within 24 hrs.

Because platforms are protected from litigation under Section 230 CDA in the US, there are less incentives for proactive moderation. Following the Christchurch incident, congressional hearings exposed how little risk gaming corporations had previously taken on extremism.

The IT Rules in India require platforms to designate compliance officers are promptly delete anything that has been detected, but enforcement capabilities are still lacking.

The majority of companies put profit before community safety, which allows radicals to take advantage of lapses in real-time moderation. Robust enforcement is hindered by legal uncertainties, economic concerns, and reputational hazards, even when AI techniques are used to detect material.

6. Case Studies related to Gaming Platforms

6.1 Modding environments and sandbox games-Players may make their own maps, servers, and mods in open world games like GTA V, Roblox, and Minecraft. By these technologies to mimic assaults and implant propaganda, extremist organisations transform violent ideology into participatory entertainment. Extremist themes get ingrained in game culture as a result of altered surroundings that normalise hatred and violence.[99]

[98] Responsible Gaming Regulations and Statutes Guide, *available at:* https://www.americangaming.org/resources/responsible-gaming-regulations-and-statutes-guide/ (last visited on October 24,2025).

[99] Virtual Worlds, Real Threats: Violent Extremist Exploitation of Roblox and Wider Gaming Ecosystems, *available at:* https://gnet-research.org/2025/09/22/virtual-worlds-real-threats-violent-extremist-exploitation-of-roblox-and-wider-gaming-ecosystems/ (last visited on 24 October,2025).

Image 1- Terrorists [Add-On Ped]- GTA 5

6.2 Communities for Competitive Gaming and Esports Extremists take advantage of the strong communities created by competitive platforms such as CS: GO and esport competitions. In discussions and live broadcast, hate speech, polarising memes, and coded messages are frequently disguising themselves as rivalry or amusement. Peer pressure reduces opposition to normalise radical discourse.

Image 2- Screenshot of Counter Strike: Global Offensive Strike (CS:GO)

6.3 social media and In-Game Communication-

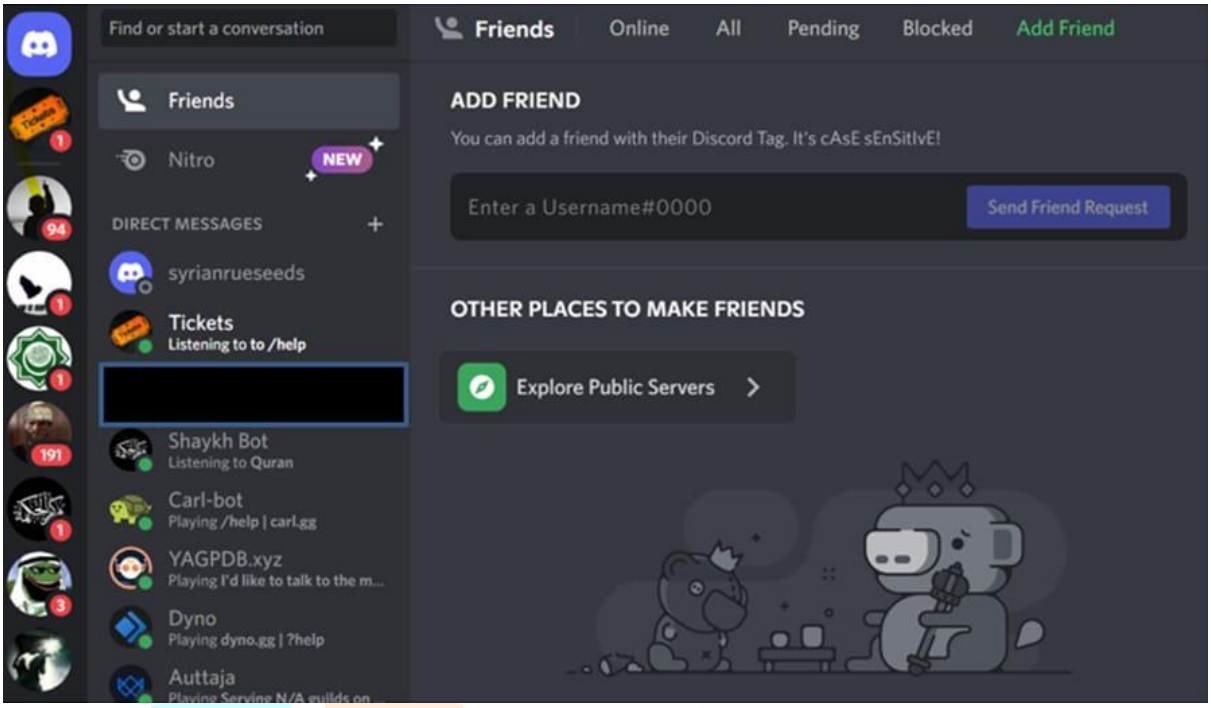


Image 3 - Screenshot of Discord interface from ISD ("Discord & Extremism")

Discord, steam, Twitch, and other chat-based platform have become into centres for extremist networking. Under the guise of a community, extremist organisation recruit, distribute material, and set up secret servers. Discord has been used to host networks connected to extremist movements of various ideologies and movements of various ideologies and to organise rallies in real life. Labels like "incel", "Nazi", or "right wing" are frequently used to identify extremist servers, making them simple for prospective members to identify. Extremist groups on Steam have utilised coded identities like 1488 and extolled former assailants. These instances demonstrate how radicalisation appears commonplace in online settings since extremist activity fits in well with gaming subcultures.[100]

7. Legal, Ethical, and Security Challenges

Significant ethical, legal, and security issues have been brought to light by the use of gaming platforms and artificial intelligence into extremist tactics. Digital surroundings, in contrast to conventional places of radicalisation, make it difficult to distinguish between extremist agitation, free expression, and enjoyment. Because platforms that support extremist activities also serve as cultural centres for millions of innocent people, this leads to a regulatory conundrum.

7.1 Legal disparities among jurisdictions- One of the main problems are that different jurisdiction have different legal systems.

European Union (EU)- Discord, Twitch, and Roblox are subject to proactive obligations under the Digital Services Act (DSA,2022) to identify and eliminate unlawful content. It expands upon previous regulations

[100] Senator to Valve: what's with all the Nazis on Steam? *available at:* https://www.theverge.com/2024/11/15/24297364/steam-extremist-content-moderation-us-senator-warner-letter (last visited on October 24,2025).

like the EU Terrorism Directive (2017/541), which makes "public provocation to commit terrorist offences" illegal and applies to propaganda or extremist gaming.

United States (US)- In contrast, platforms are protected from liability for user-generated materials by Section 230 of the Communication Decency Act 1996. The US legal system places a higher priority on free expression than proactive moderation, especially when combined with First Amendment, which protects speech unless it provokes "imminent lawless action" (Brandenburg v. Ohio, 1969).

United Kingdom (UK)- The Terrorism Act 2006 criminalise publication of terrorist content, including digital games and internet propaganda. Prosecution based on digital content have been sustained by courts, and the Online Safety Act (2023) requires tech firms to take down extremist information.

India- Authorities are empowered to restrict or remove internet information considered extremist by the Unlawful Activities (Prevention) Act and the Information Technology Rules 2021. As seen in Shreya Singhal v. Union of India, where the Supreme Court invalidated Section 66A IT Act for infringing free expression, detractors contend that these measures run the danger of overreaching even though they are successful in squelching extremist content. The difficulties of creating a unified international system is demonstrated by the differences between the US's free-speech guarantees, the EU's proactive responsibilities, and India's punitive approach.

7.2 Ethical Dilemmas: Public Safety v. Free Speech- Finding a balance between the necessity to restrict extremist discourse and the right to free speech is a recurring ethical conundrum. It may be challenging to discern coded hate speech from edgy humour in gaming discussions, esport feeds and mods. While under regulation allows extreme information to remain undetected, overregulation runs the danger of restricting free expression and stifling innovation. Questions of proportionality are raised by US cases like Holder v. Humanitarian Law Project, which show how even non-violent support for extremist groups cam be criminalised.

7.3 Risks to Security: AI, Decentralisation, and Encryption- Digital radicalisation is becoming more decentralised and international. Private or encrypted servers are offered by platforms like Discord and Steam, making surveillance challenging. Extremist cells may recruit and organise internationally thanks to encrypted communications and gaming related platforms that are hidden from law authorities. AI makes deepfake propaganda, automated hiring, and personalised grooming possible, which increases security threats. Although manipulation is acknowledged as a "high-risk" use case under the EU AI Act 2024, enforcement of this law lags behind radical innovation.

7.4 International Framework and Gaps- At the international level, the Budapest Convention on Cybercrime 2001 offers means for collaboration, while UN Security Council Resolution 2178 (20140 calls on governments to combat online terrorists recruiting. However, there is still little cross-border cooperation and uneven enforcement. In order to avoid discovery, extremist take advantage of these jurisdictional loopholes by switching between platforms and states.

8. Outcomes-

1. According to the research, radicalisation in gaming is normal development of extremist communication tactics rather than isolated phenomenon. Ideology, identity, and entertainment all converge in decentralised ecosystems that are gaming communities. The outcome is obvious, frameworks for counter-extremism must change from reactive moderation to active participation in these arenas.

2. findings show that algorithmic exposure, identity exploration, and social isolation increase youth vulnerability. Therefore, emphasis need to be placed on fostering resilience via digital literacy, emotional control, and community awareness.

3. AI is established in the study as a tool for both prevention and exploitation. As long as ethical and privacy norms are upheld, law enforcement can utilise AI for early detection, network mapping, and deradicalisation, while extremists use it for persuasion and microtargeting.

4. Instead of working alone, governments, gaming companies, parents, and youth organisations need to coordinate their activities. Collaboration across sectors is essential to striking a balance between safety and innovation.

5. As far as determining who is responsible for extremist information on gaming platforms, there is still a normative gap. This necessitates a fresh global discussion on AI governance, algorithmic transparency, and intermediary accountability.

9. Suggestions-

1. Regulations pertaining to information technology and intermediary liability should be updated by governments to specifically address online gaming sites that display user-generated content.

2. Extend the meanings of “material support” and “online dissemination” in anti-terrorism legislation to encompass extremist actions in gaming settings.

3. Regulation must strike a balance between data protection requirements under laws like India’s Digital Personal Data Protection Act 2023 and the EU Charter of Fundamental Rights, as well as security and freedom of expression.

4. Incorporate transparent, bias-audited AI techniques to identify violent-mod content, coded languages, and extremist memes in chatrooms and games.

5. Include counter-narrative and media literacy instruction in curricula at schools and universities to assist students in identifying manipulative online behaviour.

10. Conclusion-

Radicalisation has permeated young people's daily digital life and is no longer confined to lone extremist websites. Extremist organisations today take use of anonymity, community, and creative freedom on gaming platforms, esports communities, and social media sites like Discord and Twitch as a breeding ground for new members. In addition to taking over popular platforms, radicals have developed their own propaganda games and are using artificial intelligence more and more to tailor recruiting, which makes their outreach quicker, more engaging, and more difficult to identify.

Responses are still dispersed legally. India has a punitive security-heavy approach, the US priorities free speech, and the EU places a strong focus on proactive responsibility. Speech and privacy ethics continue to be problematic, and security threats are made worse by decentralised platforms and artificial intelligence. There is international framework such as UNSC Resolution 2178, however they are not enforceable. Harmonised regulations, technology protections, and culturally sensitive preventative measures are the way forward. The issue cannot be resolved by law alone, technology alone, or education alone. It is crucial to have thorough, multidisciplinary strategy that integrates ethics, technology, legislation and youth involvement.

Extreme recruiters will continue to dominate the digital frontier of gaming and artificial intelligence unless prevention advances at the same rate as extreme innovation. On the other hand, if communities, platforms, and states work together, gaming areas may change from being places for recruiting to effective resources for prevention and resilience.