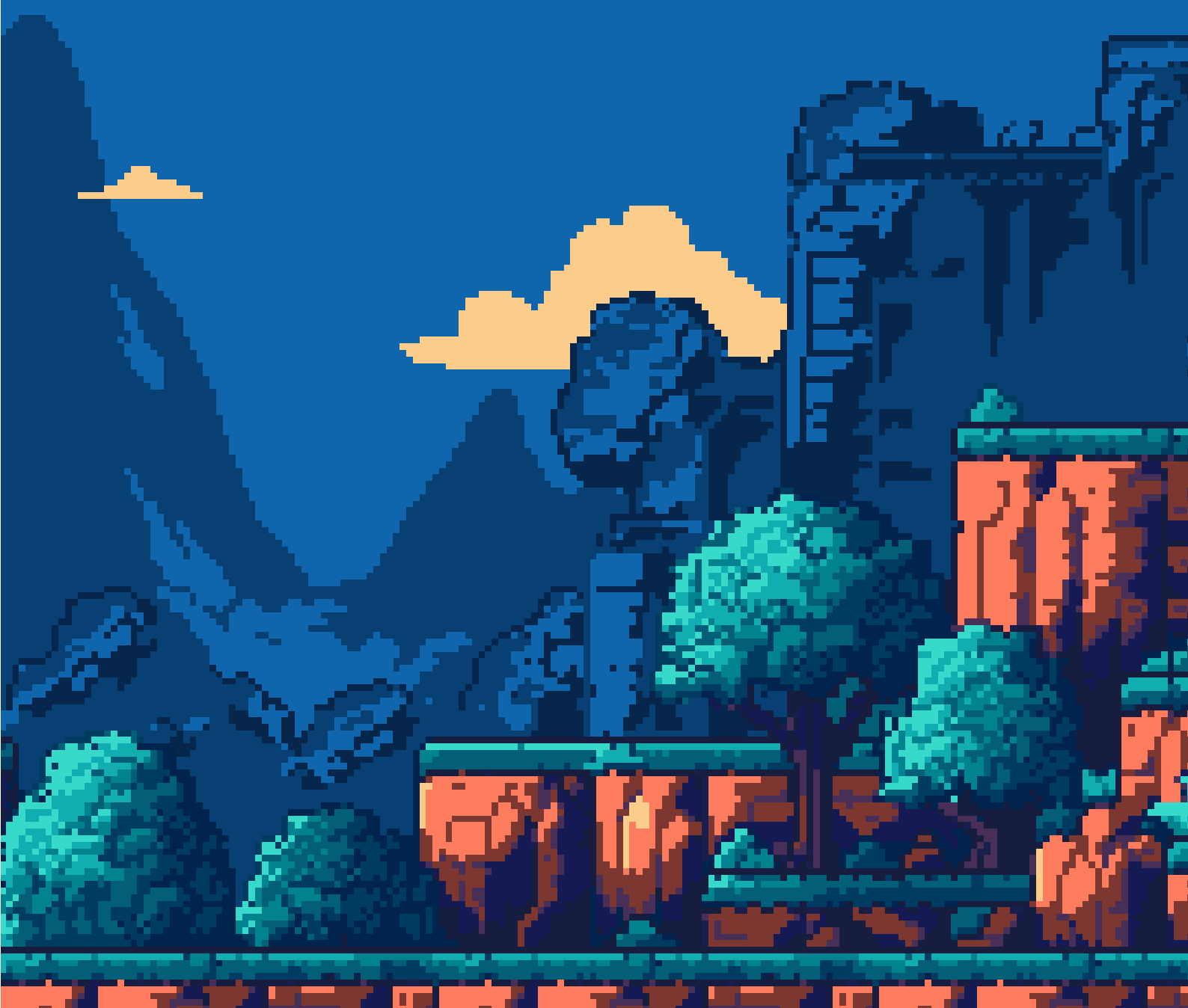
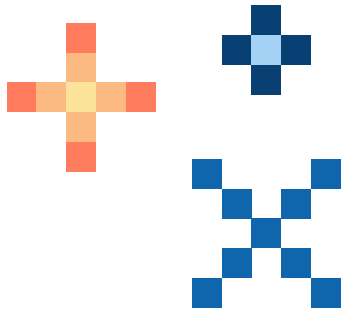


LEVEL UP

Gaming and Violent Extremism in Africa





©United Nations Interregional Crime and Justice Research Institute (UNICRI), 2025

Viale Maestri del Lavoro,10

10127 Turin, Italy

Website: www.unicri.org

E-mail: unicri.publicinfo@un.org

©United Nations Office of Counter-Terrorism (UNOCT), 2025

405 E 45th Street

New York, NY 10017

Website: www.un.org/counterterrorism/

E-mail: uncct_pcve@un.org



* **DISCLAIMER** *

The opinions, findings, conclusions and recommendations expressed herein do not necessarily reflect the views of the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Counter-Terrorism Centre (UNCCT) in the United Nations Office of Counter-Terrorism (UNOCT), or contributory organizations, and do not imply any endorsement. The content of this publication may be quoted or reproduced in part, provided that the source of information is acknowledged. UNICRI and UNOCT would like to receive a copy of the document in which this publication is used or quoted.

The designation employed and presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations and UNICRI, concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitation of its frontiers or boundaries.

* **ACKNOWLEDGEMENTS** *

This report is the product of a joint research initiative by UNICRI and UNOCT, which has been made possible with financial support from Italy. It was written by Galen Lamphere-Englund, Co-Founder, Extremism and Gaming Research Network and Consultant at both UNICRI and UNOCT, under the guidance of Odhran McCarthy (UNICRI), Sian Hutchinson and Liliane Vicente (UNOCT), with editing by Marina Mazzini (UNICRI) and design by Marianna Fassio (UNICRI). UNICRI and UNOCT wish to extend their gratitude to all the key stakeholders and partners who generously dedicated their time to be interviewed for this research. Particular thanks are due to Kentaro Matsumura, Counter-Terrorism expert at the Permanent Mission of Japan, for his continued support and enthusiasm.





* FOREWORD *

The world of gaming is one of the most dynamic and rapidly evolving digital landscapes of our time. Billions of players connect each day, from all corners of the globe, on platforms that transcend traditional national and regional borders, and push the boundaries of how we understand and experience human interaction. No longer just a form of entertainment, gaming now sits at the heart of digital culture and participatory media.

In this vein, we must equally shift our perception of gaming, from a niche activity for young people to a powerful social ecosystem – one that fosters connection, shapes identities, and can, at times, create vulnerabilities that may be exploited. As the influence of gaming continues to grow, so too must our efforts to understand the dynamics of this community, harness its positive potential, and mitigate the risks associated with its misuse.

This report, made possible through the financial support from Italy, is the product of a partnership between the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Counter-Terrorism Centre (UNCCT) at the United Nations Office of Counter-Terrorism (UNOCT), aimed at deepening understanding of gaming-related online harms, particularly in the context of violent extremism conducive to terrorism. It builds upon the foundations laid by UNOCT in its seminal 2022 study, *Examining the Intersection between Gaming and Violent Extremism*, which found that while gaming itself does not cause radicalization, violent extremist actors are increasingly seeking to exploit gaming-adjacent spaces, such as chat functions, livestreams, and user-generated content, to spread propaganda and amplify their influence. Expanding on these findings, this report offers a focused, context-sensitive analysis of trends, risks, and opportunities in Africa, the world's fastest-growing gaming community in the world. Through this lens, the report seeks to inform policy, support practitioner engagement, and catalyze cross-sector collaboration to ensure that gaming remains a force for good, and not a vector for harm.

The present study on Africa will be complemented by an additional report by UNICRI and UNOCT, focusing on Southeast Asia - home to one of the largest and most active gaming communities in the world. This second study, produced with the financial support of the Government of Australia's Department of Home Affairs, will be released in early 2026. Together, these regional studies reflect our commitment to better understand the complex relationship between gaming and violent extremism and to explore the unique cultural and linguistic dynamics of different regions and their local gamers, developers, and gaming communities.

Gaming is here to stay, along with the vibrant communities, cultures, and connections it enables. The task ahead of us is to understand how we can best protect and harness these unique and important spaces held precious by so many, not only for safety, but also for positive social connection.

We trust that this report will serve as a meaningful step towards safeguarding gaming spaces and harnessing their potential for peace, security, and development.



Alexandre Zouev

Acting Under-Secretary-General for Counter-Terrorism

United Nations Office of
Counter-Terrorism (UNOCT)



Leif Villadsen

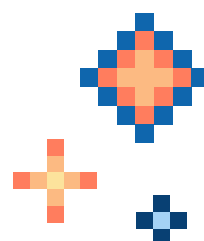
Acting Director

United Nations Interregional Crime
and Justice Research Institute (UNICRI)

* TABLE OF CONTENTS *



Executive Summary *	6
Introduction *	9
Methodology Note *	11
The Gaming Landscape in Africa *	12
Growth and Market Expansion	12
Platforms	14
Gaming Centres	15
Esports	16
Games	16
Developers and Studios	19
Online Harms and Violent Extremist Exploitation in Gaming: Scenarios for African Contexts *	22
× Scenario One: Creating New Video Games and Modifications	24
× Scenario Two: Exploiting Offline Gaming Social Environments	27
× Scenario Three: Recruiting and Communicating in Games	28
× Scenario Four: Gamifying Terrorist Content	30
× Scenario Five: Using Gaming References and Aesthetics for Propaganda	33
× Scenario Six: Financing of Terrorism and Money Laundering	35
Prevention and Resilience Building Opportunities *	39
Using Gaming for Good: Case Studies	41
× Wewe.vote – Strengthening Democratic Engagement	41
× Mission 55 – African Union Peace & Security Education	42
× Electric Blue – Wildlife Conservation Through Gaming	42
Networks	42
× Pan Africa Gaming Group (PAGG)	42
Game Jams and Summits	43
× Green Games Summit	43
× Games for Change Africa	43
× GameUp Africa Jam for Democrac	43
Other Africa-Specific Gaming Industry Platforms	44
Conclusion & Recommendations *	45





* EXECUTIVE SUMMARY *

The gaming ecosystem across Africa is at an inflection point. Smartphone penetration is soaring: 527 million mobile-phone owners in Sub-Saharan Africa in 2023 are projected to increase to 751 million by 2030, 87% of whom will own smartphones.¹ Gaming has ridden this wave: 32 million across the continent became new gamers in 2024, bringing the total to roughly 349 million players who already spend US\$1.8 billion a year on games and in-app purchases.² Analysts describe this surge bluntly: *the next billion gamers will be African*.³ With that boom and the social connectivity comes risks: Africa, and especially the Sahel, remains the most impacted by terrorism globally. Violent extremist and terrorist groups exploit the social links of gaming platforms elsewhere in the world to propagandize, radicalize individuals, and recruit new members: it is only a matter of time before they do so in rapidly digitizing African contexts.⁴

For those gamers, mobile is key: 92% of surveyed gamers in Egypt, Kenya, Nigeria, and South Africa play on mobile phones, while only 26% use tablets and 31% consoles.⁵ Notably, of the 17 most-played African titles, 13 already offer multiplayer modes and 11 provide in-game chat, turning mobile games into social networks. At the same time, “old-school” offline gaming centres persist as affordable, male-dominated social spaces that host tournaments and nurture local e-sports scenes.

To date, few verified incidents link Africa-based violent extremist groups to online gaming platforms. However, groups such as Jama’atu Ahlis Sunna Lidda’awati Wal-Jihad (Boko Haram) already use offline games to train child soldiers, and Al-Shabaab has a record of rapid tech adoption. Horizon-scanning carried out for this report adapts global Violent Extremist Organizations (VEOs) precedents of gaming use to Africa and identifies six realistic threat scenarios:

1. **Custom extremist games and modifications (user-created changes to existing games)**
2. **Recruitment in gaming cafés and mobile multiplayer lobbies**
3. **Real-time attack livestreams framed as “In Real Life (IRL) First-Person Shooter (FPS)” events**

-
- 1 Newzoo, *2024 Newzoo Free Global Games Market Report* (Newzoo, August 2024), <https://newzoo.com/games-market-reports-forecasts>.
 - 2 ITWeb, *Africa’s Gaming Market Reached \$1.8bn in 2024*.
 - 3 Pan Africa Gaming Group (PAGG Group), Homepage, 2024, <https://pagg.group/>.
 - 4 See, for example, Linda Schlegel and Rachel Kowert, eds., *Gaming and Extremism: The Radicalization of Digital Playgrounds* (Routledge, 2024), <https://www.taylorfrancis.com/books/oa-edit/10.4324/9781003388371/gaming-extremism-linda-schlegel-rachel-kowert>; Jessica White et al., *Radicalisation through Gaming: The Role of Gendered Social Identity* (Royal United Services Institute (RUSI), 2024); Galen Lamphere-Englund, 2024 *Resource List: Violent Extremism, Radicalization, and Gaming* (Global Internet Forum to Counter-Terrorism (GIFCT) and Extremism and Gaming Research Network (EGRN), 2025), <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-EG-Resources-1.1.pdf>.
 - 5 ITWeb, 2024, <https://www.itweb.co.za/article/africas-gaming-market-reached-18bn-in-2024/GxwQDM1D4GY7IPVo>; GeoPoll, *Gaming in Africa 2024: A GeoPoll Report*, GeoPoll, 2024, <https://www.geopoll.com/mobile-web-surveys/>.



4. **Gamified propaganda memes and machinima**
5. **Micro-transaction laundering via skins, keys, and crypto gateways**
6. **Violent misogyny in online gaming, including through gender-based harassment, serves as a gateway to violent extremism and weakens community resilience to radicalization to violence.**

Recruitment and propaganda pathways score medium-to-high risk; financing abuse remains lower but plausible as financial oversight tightens elsewhere.

Law-enforcement agencies generally lack investigative tools for voice, video and in-game chats, while platform moderation in African languages is limited or non-existent. Offline cafés operate without basic safeguards, and misogynistic norms common in gaming cultures create fertile ground for terrorist grooming.

Unlike North America, Europe, or South-East Asia — where VEO exploitation of gaming is already entrenched — African Member States still enjoy a narrow window to “design in” safety. The continent’s vibrant studios, e-sports federations and *gaming-for-good* initiatives (including conservation games and counter-disinformation titles) provide natural allies for preventive action. Towards that end, this report recommends a strategic response via recommendations contained at the end of this document:

1. **Prevent** – Launch a *Gaming Safety Africa Hub* to convene annual red-team exercises and fund multilingual safety resources, including risk mitigation measures for human rights infringements; certify gaming cafés that adopt age-checks, train staff and deploy helpline signage; badge “Gender-Safe Lobbies” inside top mobile titles; and add gender-responsive training for developers and game designers to mitigate violent misogyny inside games, as a known correlate to violent extremism.
2. **Detect** – Train Trusted Community Moderators (TCMs) across key markets and supply a dual-track reporting portal; develop linguistically nuanced classifiers and lexicons — for example in Hausa, Swahili, Amharic and Somali — for company and platform use.
3. **React** – Train TCMs to use a referral widget in games and in café point-of-sale systems that connects staff to regional psychosocial Non-Governmental Organizations (NGOs) within 24 hours and, where these are not available, provides de-escalation resources or connection to parallel referral systems for survivors of online harassment.



Regulators, studios, telecoms, civil-society groups, and global platforms must act **now** — before violent extremist groups exploit gaming at scale across the continent. By institutionalizing *Prevent–Detect–React* measures while the sector is still scaling, stakeholders can secure the social upside of Africa’s gaming boom and deny violent extremists a new digital front.



* INTRODUCTION *

Video games, and the communities around them, are vibrant, diverse spaces where over 3.8 billion people across the world play on a regular basis.⁶ People play games to find joy, friendships, and to build a sense of identity, all of which are pro-social acts. Yet the immense social connectivity of modern multiplayer games, livestreaming platforms and gaming-related social media – combined with the pop culture appeal of gaming – create opportunities for malign actors to exploit. Globally, terrorists and violent extremist actors have exploited gaming ecosystems for over 30 years. Their tactics range from building violently racist and xenophobic games to recreating attacks on religious sites, directly targeting gamers for recruitment via in-game chats, and taking advantage of misogynistic, racist, and insular elements of some gaming communities to radicalize members to violence. Since 2019, over nine major attacks have involved the use of gaming platforms or services.⁷

While research and policy efforts on gaming and violent extremism have increased in recent years – with 122 research pieces published since 2020 – there remains a remarkable gap in evidence at a country or regional level across African contexts.⁸ To date, no research has directly considered the intersection between gaming and violent extremism across Africa. Yet six of the ten countries most impacted by terrorism in 2024 are on the continent, particularly in the Sahel, where deaths from terrorist attacks have increased tenfold since 2019 and now account for 51% of all terrorism fatalities globally.⁹ Meanwhile, socially connected mobile gaming is booming, with the player base expanding by nearly 10% in 2024 alone, underscoring the continent's rapid growth in the sector.¹⁰ The United Nations Interregional Crime and Justice Research Institute (UNICRI) and the Office of Counter-Terrorism (UNOCT) have partnered to develop this focused research, building on UNOCT's prior report, 'Examining the Intersection Between Gaming and Violent Extremism', which explored terrorist and violent extremist exploits of the Internet,

6 Newzoo, *2024 Newzoo Free Global Games Market Report* (Newzoo, August 2024), <https://newzoo.com/games-market-reports-forecasts>.

7 Linda Schlegel and Rachel Kowert, eds., *Gaming and Extremism: The Radicalization of Digital Playgrounds* (Routledge, 2024), <https://www.taylorfrancis.com/books/oa-edit/10.4324/9781003388371/gaming-extremism-linda-schlegel-rachel-kowert>; Jessica White et al., *Radicalisation through Gaming: The Role of Gendered Social Identity* (Royal United Services Institute (RUSI), 2024); Galen Lamphere-Englund, *2024 Resource List: Violent Extremism, Radicalization, and Gaming* (Global Internet Forum to Counter-Terrorism (GIFCT) and Extremism and Gaming Research Network (EGRN), 2025), <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-EG-Resources-1.1.pdf>.

8 Galen Lamphere-Englund, *2024 Resource List: Violent Extremism, Radicalization, and Gaming* (Global Internet Forum to Counter-Terrorism (GIFCT) and Extremism and Gaming Research Network (EGRN), 2025).

9 Institute for Economics & Peace, *Global Terrorism Index 2025: Measuring the Impact of Terrorism* (Sydney: Institute for Economics & Peace, March 2025), <https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf>.

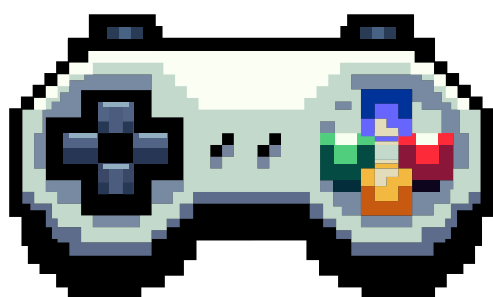
10 Carry1st and Newzoo, "Africa's Gaming Market Reaches \$1.8bn; Sixfold Growth vs. ROW Driven by 32mn New Gamers in 2024," February 5, 2025, <https://www.carry1st.com/press/africas-gaming-market-reaches-1-8bn-sixfold-growth-vs-row-driven-by-32mn-new-gamers-in-2024>.



social media, and gaming surfaces globally from a gamer's perspective.¹¹ In doing so, UNICRI and UNOCT seek to contextualize harms across gaming platforms in countries across Africa.

This report draws on a global research review and interviews with industry, youth, and preventing and countering violent extremism (PCVE) practitioners to present an overview of the current gaming landscape and ecosystem across Africa, including both Sub-Saharan Africa and North Africa. It then reviews known terrorist and violent extremist exploits of gaming platforms and services from other regions, and uses these to develop scenarios illustrating how such threats might manifest in the African areas most impacted by terrorist activity – namely the Sahel, East Africa, and Horn of Africa. The research also explores how games are already being used to build resilient communities and foster positive social change – building on work from Games for Change Africa and the Pan-Africa Gaming Guild (PAGG) – to provide recommendations for how those risks might be mitigated.

For practical purposes, this report focuses on horizon scanning and scenario mapping to provide a map of potential exploits. It is not intended to be a comprehensive all-source report. Instead, by drawing on known cases of terrorist and violent extremist uses of gaming platforms and services from elsewhere in the world and applying insights from interviews and activity patterns of violent extremist groups, it presents explicit threat models to protect against. The Swedish Psychological Defence Agency and Lund University have taken a similar approach to model threat scenarios, namely by discussing specific tactics, techniques, and procedures that could be used by foreign malign influence operations on gaming surfaces.¹² This format is used for inspiration here. Future research, such as polling around existing exposure to terrorist and violent extremist harms, radicalization to violence patterns, and in-depth platform data may well illustrate current exploits taking place.



-
- ¹¹ Linda Schlegel and Amarnath Amarasingam, *Examining the Intersection Between Gaming and Violent Extremism* (United Nations Office of Counter-Terrorism (UNOCT), 2022), <https://www.un.org/counterterrorism/Examining-the-Intersection-Between-Gaming-and-Violent%20Extremism>; United Nations Interregional Crime and Justice Research Institute (UNICRI) and United Nations Office of Counter-Terrorism (UNOCT), *Beneath the Surface: Terrorist and Violent Extremist Use of the Dark Web and Cyber-crime-as-a-Service for Cyber-Attacks* (2024), https://unicri.it/sites/default/files/2024-07/DW_BtS.pdf.
- ¹² James Pamment, Jesper Falkheimer, and Elsa Isaksson, *Malign Foreign Interference and Information Influence on Video Game Platforms: Understanding the Adversarial Playbook* (Lund University and Swedish Psychological Defense Agency, 2023), <https://www.mpf.se/publikationer/publikationer/2023-12-01-malign-foreign-interference-and-information-influence-on-video-game-platforms-understanding-the-adversarial-playbook>.



* METHODOLOGY NOTE *

This report provides both an overview of the gaming industry and terrorist and violent extremist trends across Africa, and a forward-looking review of gaming, radicalization to terrorism and violent extremism conducive to terrorism. This study is indicative and not representative in nature. Research was conducted from January to May 2025. As such, the abbreviated qualitative methodological approach draws on:

- ✖ A desk review of over 160 academic and grey sector articles and reports related to gaming and violent extremism, accessible via the EGRN Gaming and Extremism Library,¹³ 12 reports covering the recent state of gaming studios and industry on the continent, and additional literature from terrorism and conflict studies to contextualize non-state armed group (NSAG), terrorist and violent extremist activities in Sub-Saharan Africa.
- ✖ Key informant interviews with gaming developers (two male respondents), gaming platform staff (one female respondent), and government representatives (one male respondent).
- ✖ A focus group discussion with young gamers from UNOCT's Youth Engagement and Empowerment Alumni from Nigeria and Kenya (two male respondents and one female respondent).
- ✖ Scenario modelling based on documentation of known terrorist and violent extremist activity in other regions of the world, including the adoption of gaming platforms for game production, propagandizing and gamifying attacks, recruitment and communication, radicalization and socialization into violence, and terrorism financing.¹⁴

¹³ Lamphere-Englund, 2024 Resource List: Violent Extremism, Radicalization, and Gaming.

¹⁴ See overview of these categories here: Galen Lamphere-Englund and Jessica White, The Online Gaming Ecosystem: Assessing Digital Socialization, Extremism Risks and Harms Mitigation Efforts (Extremism and Gaming Research Network (EGRN) and the Global Network on Extremism and Technology (GNET), 2023), https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf.

* THE GAMING LANDSCAPE IN AFRICA *

"The Next Billion Gamers Will be African" (Gaming Industry Interview #1, 2024).

People playing video games and local and global industries developing them are rapidly expanding across Africa. The continent is viewed by many analysts as the most important emerging market for the sector, with smartphone (mobile) gaming surging alongside smartphone adoption and improved Internet access. Local game studios are also creating innovative indie games – smaller independent titles developed outside the most prominent studios – while major international developers are working to localize their approaches.

Growth and Market Expansion

Population growth across the incredibly diverse continent of Africa remains among the highest in the world. Despite generally declining birth rates, an estimated 1.53 billion people live across the continent in 2025. They will increase to 1.73 billion in 2030, when approximately one in five people worldwide will live in Sub-Saharan Africa (SSA).¹⁵ The median age across the continent is 19.2, with half the population younger.¹⁶ At the same time, and with increased development, access to the Internet and smartphones is dramatically improving. The mobile phone industry body, GSMA, estimates that some 527 million mobile phone subscribers and 320 million mobile Internet users lived in SSA¹⁷ in 2023, the most recent year for which disaggregated estimates were available. Five years from now, in 2030, 751 million people in Sub-Saharan Africa will have a mobile phone, and 518 million will be online.¹⁸ According to the same study, GSMA estimates that over 87% of the population in Sub-Saharan Africa will own a smartphone by 2030. Affordability and data access remain challenging for some countries and demographics, but access trends are changing. These demographic shifts, along with Internet and smartphone access, are rapidly bringing new generations online and, with that connectivity, a desire to play Internet-connected video games on their devices. Historically, games on smartphones have not had multiplayer functionalities, and have mostly been accessed through well-regulated app stores (Google Play Store and the Apple App Store). However, the latest generation of mobile games are extremely socially connected, multiplayer, and increasingly available through other stores or platforms (via .APK downloads for Android, for example). Worldwide, some 3.42 billion people played video games in 2024, growing at a pace of 4.5%

15 United Nations Department of Economic and Social Affairs, Population Division, "The Outlook for Population in Africa," *Japan Economic Foundation SPOTLIGHT*, no. 253 (January/February 2024): 60-62, https://www.jef.or.jp/journal/pdf/253rd_Special_Article_04.pdf.

16 Worldometer, "Africa Demographics 2024," Worldometer, accessed March 5, 2025, <https://www.worldometers.info/demographics/demographics-of-africa/>.

17 Note: GSMA, the main industry body publishing figures on mobile phones and internet access, groups their reports into North Africa and the Middle East (MENA) and Sub-Saharan Africa, making continent-wide figures difficult to approximate.

18 GSMA, *The Mobile Economy Sub-Saharan Africa 2024* (GSMA, 2025), https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/11/GSMA_ME_SSA_2024_Web.pdf.

year-on-year (YOY).¹⁹ Across Africa, meanwhile, 32 million people became new gamers in 2024 – a 10% increase from the prior year – bringing the total gamers across the continent to 349 million.²⁰ Recent polling from Egypt, Kenya, Nigeria, and South Africa found no significant gender divide among those playing games (49% female and 51% male).²¹ Demographics skewed younger than global average – as expected, given the continent’s lower median age – with roughly 28% aged 15-24, 38% aged 25-34, and 34% aged 35 or older.²²

Gaming markets across Africa were valued at US\$1.8 billion in revenue in 2024, and are projected to exceed US\$2.5 billion by 2028.²³ While this still represents a small share of the US\$188 billion in global gaming industry revenues, growth in African markets outpaces global levels by a factor of six: 12.4% YOY revenue growth across the continent compared with the global average of 2.1% between 2023-2024.²⁴ This stands in contrast to gaming audiences in most of the world, where markets are maturing and YOY revenue growth has slowed to single digits across Asia-Pacific, Europe, and North America.

Based on projections from Carry1st, the largest publisher of games on the continent, and Newzoo, a gaming data provider, the African countries with the highest annual gaming revenue were Egypt (US\$386 million), Nigeria (US\$300 million), and South Africa (US\$278 million). Eritrea and Niger were identified as the fastest-growing markets, while Equatorial Guinea and the Seychelles were the slowest.²⁵ Complementary figures from 2024, focusing only on in-app purchases from mobile games on Android and iOS, ranked South Africa as the leading country in revenue (US\$111.9 million), followed by Nigeria (US\$60.9 million), Egypt (US\$39.1 million), Algeria (US\$8.0 million), and Tunisia (US\$6.4 million).²⁶ Interestingly, gaming revenues in Nigeria increased six fold between 2019 and 2024, while revenues in other countries declined, particularly in North Africa. These figures suggest that the continent’s prime gaming markets may be shifting from North Africa towards Southern states.

19 Newzoo, *2024 Newzoo Free Global Games Market Report* (Newzoo, August 2024), <https://newzoo.com/games-market-reports-forecasts>.

20 Carry1st and Newzoo, *Africa’s Gaming Market Reaches \$1.8bn: Sixfold Growth vs. ROW Driven by 32mn New Gamers in 2024* (2025).

21 GeoPoll, *Gaming in Africa 2024* (GeoPoll, 2024), <https://www.geopoll.com>.

22 Ibid.

23 Carry1st and Newzoo, *Africa’s Gaming Market Reaches \$1.8bn: Sixfold Growth vs. ROW Driven by 32mn New Gamers in 2024* (Carry1st and Newzoo, 2025), <https://www.carry1st.com/press/africas-gaming-market-reaches-1-8bn-sixfold-growth-vs-row-driven-by-32mn-new-gamers-in-2024>

24 Newzoo, *2024 Newzoo Free Global Games Market Report* (Newzoo, August 2024), <https://newzoo.com/games-market-reports-forecasts>; Perry Gresham, Mark Qi, and Rhys Elliott, *MIDiA Research Global Games Forecasts 2025–2031: The Market Is Mature, So Double-Digit Growth Is a Fantasy* (London: MIDiA Research, January 2025), <https://www.midiaresearch.com/games-forecasts>.

25 Ibid.

26 Maliyo Games, *2025 Africa Games Industry Report* (Lagos: Maliyo Games, 2025), <https://www.africagamesreport.com>.



Platforms

Mobile phones dominate the continent's gaming landscape. Gamers across Africa overwhelmingly play on smartphones: interviews with African gaming industry insiders indicate that the majority of their audiences are on these devices. Polling in 2024 among 2,588 gamers in Egypt, Kenya, Nigeria, and South Africa confirmed that 92% of respondents played games regularly on mobile phones, while 51% played on computers, 31% on game consoles, and just 26% on tablets.²⁷ Notably, the vast majority of handsets in use across Africa are Android-based (85.74% market share) compared with Apple's iOS (13.29% market share).²⁸ In line with this trend, mobile phones account for some 55% of global gaming software revenue, but represent the lion's share of revenue across the continent. Of the US\$1.8 billion generated in revenue by African gaming markets in 2024, approximately US\$1.6 billion (89%) came from mobile games.²⁹

Meanwhile, a review of Steam user data across 749 million accounts found that only 1.9 million were geographically tagged as being in countries across Africa.³⁰ The top ten countries with Steam accounts on the continent were:

Country Ranking by Steam Users	Country	Number of Steam Users
50	South Africa	238,777
54	Algeria	206,921
62	Egypt	163,761
65	Niger	140,998
70	Zimbabwe	120,850
81	Uganda	89,064
82	Morocco	86,463
91	Tunisia	65,630
94	Angola	64,811
106	Nigeria	52,089

²⁷ GeoPoll, *Gaming in Africa 2024* (GeoPoll, 2024), <https://www.geopoll.com>.

²⁸ StatCounter, *Mobile Operating System Market Share in Africa*, accessed March 5, 2025, <https://gs.statcounter.com/os-market-share/mobile/africa>.

²⁹ Ibid.

³⁰ World Population Review, *Steam Users by Country in 2025*, (World Population review using Steam User Map data), <https://world-populationreview.com/country-rankings/steam-users-by-country>.

Gaming Centres

Additionally, and in contrast to many other regions, gaming centres where individuals pay to play consoles and personal computers (PCs) are a central part of the industry landscape. These often relatively informal establishments give access to gaming hardware for those unable to afford personal devices, fostering communal gaming experiences. Despite the rapid proliferation of smartphones, these gaming centres remain an important feature of Africa's gaming ecosystem. In the early 2000s, gaming centres and internet cafés flourished in urban areas across North America and Europe, offering console gaming experiences on a pay-to-play basis. These venues were especially popular among young people seeking entertainment and social interaction. Today, many of the 51% of gamers on the continent who play games on computers and the 31% who play on consoles may do so through gaming centres. Our focus group respondents also noted that gaming centres in Nigeria and Kenya serve as communal hubs where gamers participate in local tournaments, socialize, and share gaming strategies.

These hybrid offline social spaces are often male-dominated and, while forming positive pro-social bonds, were flagged by our respondents as potential recruitment spaces for non-state armed groups and violent extremist (VE) groups. This is particularly notable given recent research that has demonstrated strong links between support for misogyny and support for violent extremism, with surveys in the UK, Bangladesh, Libya, Indonesia, and the Philippines showing that men supporting misogyny are up to three times more likely to support violent extremism when compared with those who do not.³¹ The proliferation of violently misogynistic norms, harassment, and bullying in gaming spaces also gives rise to significant gendered harms and creates an environment in which such norms and behaviours can undermine resilience against violent extremism.³² Violent misogyny can, in and of itself, constitute a form of violent extremism;³³ while men and boys who support it are up to three times more likely to endorse other forms of violent extremism.³⁴ Thus, misogyny constitutes a pathway to radicalization into violence, including through online video games. Elements of this are further elaborated in the scenario section of the report.

31 Bettina Rottweiler, Caitlin Clemmow, and Paul Gill, "A Common Psychology of Male Violence? Assessing the Effects of Misogyny on Intentions to Engage in Violent Extremism, Interpersonal Violence and Support for Violence against Women," *Terrorism and Political Violence*, vol. 37, no. 2 (April 3, 2025): 287–312, <https://doi.org/10.1080/09546553.2023.2292723>; Melissa Johnston and Jacqui True, *Misogyny & Violent Extremism: Implications for Preventing Violent Extremism* (Melbourne: Monash University, October 14, 2019), https://arts.monash.edu/_data/assets/pdf_file/0007/2003389/Policy-Brief_VE_and_VAW_V7t.pdf;

Galen Lamphere-Englund, Hamonangan Amores, and Farah Putri, *Pathways of Resilience to Violent Extremism in Indonesian Higher Education: A Mixed Method Study Using the Building Resilience Against Violent Extremism (BRAVE) Approach* (Jakarta: USAID Harmoni, 2022), <https://www.crisconsortium.org/research-reports-pathways-to-resilience>.

32 Cynthia Miller-Iddiss, "Misogyny Incubators: How Gaming Helps Channel Everyday Sexism into Violent Extremism," *Frontiers in Psychology*, Sec. Media Psychology, vol. 16 (2025); Jessica White et al., *Radicalisation Through Gaming: The Role of Gendered Social Identity* (Royal United Services Institute (RUSI), 2024). <https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2025.1537477/abstract>;

33 Institute for Strategic Dialogue, *Misogynistic Pathways to Radicalisation: Recommended Measures for Platforms to Assess and Mitigate Online Gender-Based Violence*. (2025); <https://www.isdglobal.org/isd-publications/misogynistic-pathways-to-radicalisation-recommended-measures-for-platforms-to-assess-and-mitigate-online-gender-based-violence>

34 Bettina Rottweiler, Caitlin Clemmow, & Paul Gill, "A Common Psychology of Male Violence? Assessing the Effects of Misogyny on Intentions to Engage in Violent Extremism, Interpersonal Violence and Support for Violence Against Women," *Terrorism and Political Violence*, vol. 37, no. 3 (2025).

Esports, referring to structured competitive gaming, are also emerging across the continent with numerous countries establishing official organizations and a growing number of tournaments, teams, and professional players. With that rise, some gaming centres have evolved to host competitive gaming events, nurturing local talent and offering platforms for practice and competition.³⁵ The Africa Esports Championship, for example, operates in 24 Member Countries, while the International Esports Federation World Championship counts federations in 30 African nations.³⁶ South Africa, in particular, has participated in every International Esports Federation World Championship since 2009, with local organizations like Mind Sports South Africa (MSSA) integrating esports into educational institutions, with over 60 schools reportedly participating in official leagues. In Kenya, Ghana, and Namibia, esports are particularly popular, with new leagues rapidly emerging.

Games

As most play takes place on smartphones, popular titles are mobile-centric. Continent-wide figures are not readily available due to a lack of disaggregated data. Still, at least across Egypt, Kenya, Nigeria, and South Africa, the following were ranked as the most popular in 2024:³⁷

1. **Candy Crush** – The famous tile-matching puzzle game.
2. **PUBG** (Most likely PUBG Mobile) – A multiplayer battle royale game.
3. **FIFA** (Potentially FIFA Mobile) – A multiplayer football title.
4. **Dream League Soccer** – An Android soccer simulator with single and multiplayer modes.
5. **Temple Run** – A runner video game built for mobile.
6. **Monopoly** – A mobile adaptation of the classic board game with multiplayer options.
7. **Call of Duty** – The world's most popular first-person shooter video game, now released for mobile with multiplayer functionality.
8. **Need for Speed** – A racing game with single and competitive multiplayer options.

35 Mordor Intelligence, *Africa Gaming Market Report*, accessed March 6, 2025, <https://www.mordorintelligence.com/industry-reports/africa-gaming-market>.

36 Africa Esports Championship, "About Us," accessed March 6, 2025, <https://aec.africa/about-us/>; International Esports Federation, "Members," accessed March 6, 2025, <https://iesf.org/members/>.

37 GeoPoll, *Gaming in Africa 2024*, <https://www.geopoll.com>.

9. **Solitaire** – The card game.
10. **Free Fire** – A battle royale shooter game with multiplayer arenas.
11. **Roblox** – The most popular platform globally for user-generated games and social multiplayer experiences across genres, focused on young users.
12. **Royal Match** – A tile-matching puzzle game with competitive events and social leaderboards.
13. **Lords Mobile** – A real-time strategy and RPG hybrid with massive multiplayer guild wars.
14. **EA Sports FC** – EA's rebranded football title with head-to-head multiplayer matches and live events.
15. **eFootball** – Konami's football simulation game offering online competitive and cooperative play.
16. **8 Ball Pool** – A casual, competitive billiards game with real-time multiplayer duels and tournaments.
17. **Yalla Ludo** – A social board game app featuring multiplayer Ludo and Domino with integrated voice chat.

Some of these titles use little to no data, helping uptake in areas with poor connectivity, while others are data-heavy multiplayer titles often played on hotspots or in areas with better internet access. Findings from the industry-led 2025 Africa Games Report, based on revenue data from Algeria, Egypt, Nigeria, Tunisia, and South Africa broadly align with the list above. However, they also include Roblox in third place by revenue, along with Candy Crush and PUBG Mobile. Royal Match (a puzzle game), Lords Mobile (a single and multiplayer strategy game), and two additional football games (EA Sports FC and eFootball) also featured in the rankings.³⁸

In reviewing which popular titles have multiplayer functions that could be exploited by malign actors, it was found that of the 17 most popular games played on the continent, 13 feature multiplayer modes, while 11 include in-game chat functionalities. Mobile multiplayer offers quick, accessible gameplay with simplified controls and shorter session lengths, ideal for casual or on-the-go users. However, limited in-game communication tools and reliance on touchscreen input reduce coordination and the depth of interaction compared to PC or console play (though this is beginning to shift). Mobile games often

38 Maliyo Games, 2025 Africa Games Industry Report, <https://www.africagamesreport.com>.



still support global matchmaking with players around the world, fostering a social ecosystem. Only four games — Candy Crush, Temple Run, Solitaire, and Royal Match — are strictly single-player with no chat functionalities. Mobile games have now evolved into sophisticated multiplayer experiences.

Game	Multiplayer Mode	In-Game Chat
Candy Crush	No	No
PUBG Mobile	Yes	Yes
FIFA Mobile	Yes	Yes
Dream League Soccer	Yes	No
Temple Run	No	No
Monopoly	Yes	Yes
Call of Duty Mobile	Yes	Yes
Need for Speed	Yes	Varies
Solitaire	No	No
Free Fire	Yes	Yes
Roblox	Yes	Yes
Royal Match	No	No
Lords Mobile	Yes	Yes
EA Sports FC	Yes	Yes
eFootball	Yes	Yes
8 Ball Pool	Yes	Yes
Yalla Ludo	Yes	Yes



Developers and Studios

The games industry is a multi-layered ecosystem – the US\$188 billion in global annual revenue comes through many streams. Across Africa, the uptake of gaming-related platforms such as Discord is growing rapidly, alongside legacy social media platforms such as Facebook and TikTok. For an overview, please see below:³⁹

Type	Description	Key Actors / Examples
Game Studios and Developers	Companies that create, design, and develop video games, ranging from independent small teams to larger studios.	African examples: Maliyo Games, Kiro'o Games, Leti Arts, Free Lives, Usiku Games, Jiwe Studio Global examples: Riot Games, CD Projekt Red
Game Publishers	Entities that finance, market, and distribute games; often supporting smaller developers to reach regional and global markets.	African examples: Carry1st, Qene Games, Africa Game Publishers Global examples: Activision Blizzard, Sony Interactive Entertainment, Tencent Games, Nintendo, Valve Corporation, Take-Two Interactive, Bethesda Softworks, Electronic Arts (EA), Ubisoft
Game Markets	Online platforms and digital stores where African gamers purchase or download video games, often integrated with payment solutions and/or social network elements tailored to local markets.	African examples: Carry1st Shop, Gamsole Global examples: Google Play Store, Apple App Store, Steam, GOG.com, itch.io, GameFly, Epic Games Store
Livestreaming Platforms	Platforms used by gamers to broadcast gameplay live, allowing real-time interaction and community building.	Global examples: Twitch, Facebook Gaming, YouTube Gaming, TikTok Live, Trovo

³⁹ Galen Lamphere-Englund and Jessica White, *The Online Gaming Ecosystem: Assessing Digital Socialization, Extremism Risks and Harms Mitigation Efforts* (Extremism and Gaming Research Network (EGRN) and the Global Network on Extremism and Technology (GNET), 2023), https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf.

Video Platforms	Peer-to-peer platforms for uploading and viewing gaming-related videos, including reviews, gameplay, and influencer content.	Global examples: YouTube, Vimeo, Utreon, Dailymotion, DTube, Instagram Reels, TikTok, PeerTube, Odysee, LBRY, Bitchute
Gaming Forums, Messaging Platforms, User-Generated Content Servers	Social spaces widely utilized across the internet where gamers discuss games, share user generated content/mods, and coordinate gaming sessions or tournaments.	Africa Examples: Reddit (r/AfricaGaming), Nairaland (Nigeria), Facebook Groups (e.g., Naija Gamer) Global examples: Discord, Telegram, WhatsApp Groups, IGN Boards, Minecraft Forum, GameFAQs, Steam, 4chan, 8Kun, Kiwifarms, Nexus Mods, ModDB
Gaming Media and Publication	Online and print media that provide news, reviews, and analysis of gaming industry development.	African examples: IGN Africa, Pulse Africa Global examples: PC Gamer, The Verge, Edge Magazine, Metacritic,
Esports Teams and Leagues	Organized competitive gaming teams and tournaments within African gaming communities.	African examples: Lagos Esports Forum, Ghana Esports Association, Africa Esports Championship (AEC), Esports Federation of Kenya Global examples: Team Liquid, OG, FaZe Clan, Team Spirit, G2 Esports
Hardware Manufacturers	Providers and distributors of gaming consoles, accessories, and equipment.	African examples: Transsion Holdings (distributor of Chinese-made Tecno, Infinix, Itel phones popular for mobile gaming), Microsoft Xbox (Africa distribution), Sony PlayStation Africa, Samsung Africa Global examples: Nvidia, Intel, AMD, Oculus, Razer, Nintendo

While Africa is not home to many hardware manufacturers or large-scale gaming platforms, the continent nonetheless hosts a significant number of studios, developers, and publishers. Most indie or independent studios are not affiliated with major publishers. At the same time, the games industry is experiencing rapid growth, with more than 250 game studios now based across Africa. Data from the African Games Developer Survey illustrates that, between 2023 and 2024, the number of studios in West Africa rose from 12 to 57 (a nearly five-fold increase); in Southern Africa from 5 to 35 (a seven-fold increase); and in East Africa from 8 to 24 (a three-fold increase). Even in Central and North Africa the number of studios grew,

from 1 to 8 and from 1 to 6 respectively. In 2024, the United Kingdom opened its first continent-focused studio.⁴⁰ An assortment of gaming studios and companies from the continent includes:

- ✖ South Africa: Pineapple on Pizza, Sea Monster Entertainment, and Carry1st (large publisher and game payment processor)
- ✖ Cameroon: Kiro'o Games and Noohkema Interactive
- ✖ Nigeria: Maliyo Games and Dimension 11
- ✖ Ghana: Leti Arts and Bawala Studios
- ✖ Senegal: Kayfo Games and Masseka Game Studio
- ✖ Kenya: Kunta Content and Daniel Macharia

According to data from Games Industry Africa and Video Games Insight, PC game releases from African game developers are increasing annually, with 16 new games launched in 2024.⁴¹ Pricing for comparable titles on Steam, the largest PC games marketplace, tends to be modest in line with market expectations, with a quarter launched over the last decade being free to play, 37% less than US\$5, and 35% less than US\$20. Over two-thirds of titles by African developers make less than US\$5,000 in lifetime revenue, but a few are more profitable: 8% of games generated over US\$1 million and 6.7% generated between US\$200,000 and US\$1 million. The most popular titles – by sales – for African developers on PC from 2020 to 2024 were *West Hunt* (2022, Tunisia, Studio: *NewGen*), *Terra Nil* (2023, South Africa, Studio: *Free Lives*), and *Anger Foot* (2024, South Africa, Studio: *Free Lives*).

The industry also includes a range of federations and industry bodies, including Games Industry Africa and the Pan-African Gaming Group (PAGG), which is dedicated to gaming for good on the continent, a key aspect of gaming further elaborated throughout the report.



⁴⁰ Maliyo Games, *2025 Africa Games Industry Report*, <https://www.africagamesreport.com>.

⁴¹ Games Industry Africa and Video Game Insights, "State of the African Games Industry 2025 – PC Edition," *Games Industry Africa*, January 29, 2025, <https://gamesindustryafrica.com/2025/01/29/state-of-the-african-games-industry-2025-pc-edition/>.



* **ONLINE HARMS AND VIOLENT EXTREMIST EXPLOITATION IN GAMING: SCENARIOS FOR AFRICAN CONTEXTS** *

The burgeoning gaming industry, smartphone-enabled multiplayer games, and broader gaming ecosystem across Africa are exciting and speak to the impressive development of digital economies. However, the social connectivity afforded by modern gaming brings with it the potential for exploitation by terrorists, violent extremists, and non-state armed actors. Other regions of the world, from North America to Europe



and Asia-Pacific, where video games have become a primary method of socialization, community building, and engagement, have seen a range of online harms related to targeted hate, toxicity, radicalization to violence, and violent extremism when conducive to terrorism. Given the widespread nature of terrorist activity and NSAGs in the Sahel, the Horn, Central Africa, and East Africa, as well as the tendency of terrorist and violent extremist actors to be early experimenters and adopters of technologies, those harms are likely to eventually become present across much of Africa.

As noted, the Sahel was the most impacted region of the world by terrorism-related fatalities in 2024, accounting for over half of all terrorism-related deaths, and has also been the most lethal conflict zone



on the continent for four years in a row.⁴² An estimated 25,000 people died in the Sahel alone as a result of conflicts in 2025, with deaths in Niger rapidly increasing and instability in the region persisting, especially in Mali and Burkina Faso. Recent attacks in Togo also raise concerns over knock-on implications for regional stability. Jama'at Nasr al-Islam wal-Muslimin (JNIM) remains the primary conflict actor in West Africa, along with IS-Sahel. In contrast, Boko Haram and Islamic State West Africa (ISWA) remain concerns and are in conflict with each other, exacerbating the existing cycle of violence. Al-Shabaab, a terrorist group in East Africa operating mainly out of Somalia and into Kenya, was the fourth most deadly terrorist group in 2024 despite significant gains in stability by the Somali state, according to the annual Global Terrorism Index published by the Institute for Economics and Peace (IEP).⁴³ Continent-wide, Burkina Faso was the most impacted by terrorism, followed by Mali (4th globally), Niger (5th), Nigeria (6th), Somalia (7th), Cameroon (10th), Democratic Republic of the Congo (12th), Mozambique (17th), and Kenya (19th).⁴⁴ However, the picture across the continent is highly dichotomous when it comes to peace: 23 countries across Africa did not record a single terrorist incident in the last five years.

Far from being a point to stoke moral panic around games, the current conflict realities in parts of Africa, combined with the rapid growth of gaming, should instead be viewed as a call to safeguard gaming spaces across the entire continent, build resilience in gaming communities, and inoculate emerging gamer spaces against violent extremism. Indeed, games provide pro-social opportunities for community development and resilience that ought to be nurtured.

To better understand the potential harms – illustrated through a series of horizon-scanning scenarios below – this report draws on over 120 resources published over the last five years, along with primary interviews carried out for this study, that document the primary ways in which violent extremist and terrorist actors are known to manipulate gaming environments.⁴⁵ Notably, this report did not conduct in-country data collection to evidence potential examples of terrorist exploitation of games currently taking place due to resource constraints. There is no openly available reporting at the time of publication suggesting that terrorist groups are doing so, yet evidence from other regions of the world suggests that uptake will likely follow adoption of gaming and gaming-adjacent platform use. Drawing on work from UNOCT, the Extremism and Gaming Research Network (EGRN), and the EU Radicalization Awareness

42 Africa Center for Strategic Studies, "Militant Islamist Groups in Africa Sustain High Pace of Lethality," *Africa Center for Strategic Studies*, February 18, 2025, <https://africacenter.org/spotlight/mig2025-militant-islamist-groups-in-africa/>; Institute for Economics & Peace, *Global Terrorism Index 2025: Measuring the Impact of Terrorism* (Sydney: Institute for Economics & Peace, March 2025), <https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf>.

43 Institute for Economics & Peace, *Global Terrorism Index 2025: Measuring the Impact of Terrorism* (Sydney: Institute for Economics & Peace, March 2025), <https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf>.

44 Ibid.

45 For example, see this resource list: Galen Lamphere-Englund, *2024 Resource List: Violent Extremism, Radicalization, and Gaming* (Global Internet Forum to Counter-Terrorism (GIFCT) and Extremism and Gaming Research Network (EGRN), 2025), <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-EG-Resources-1.1.pdf>. Other recent pieces include: Linda Schlegel and Rachel Kowert, eds., *Gaming and Extremism: The Radicalization of Digital Playgrounds* (Routledge, 2024), <https://www.taylorfrancis.com/books/oa-edit/10.4324/9781003388371/gaming-extremism-linda-schlegel-rachel-kowert>; Jessica White et al., *Radicalisation through Gaming: The Role of Gendered Social Identity* (Royal United Services Institute (RUSI), 2024); Galen Lamphere-Englund, *Prevent, Detect, and React: A Framework for Countering Violent Extremism on Gaming Surfaces* (Global Internet Forum to Counter-Terrorism (GIFCT), 2025), <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-PDR-Surfaces-1.1.pdf>.



Network (RAN, now called the Knowledge Hub), a six-part typology outlined below groups the primary hierarchy of harms posed by those actors:

1. **Creating New Video Games and Modifications (Mods)**
2. **Exploiting Gaming Social Environments**
3. **Recruiting and Communicating in Games**
4. **Gamifying Terrorist Content**
5. **Using Games for Propaganda**
6. **Financing and Money Laundering**

The scenarios below draw on known exploits from global groups falling under each use case, albeit modified to reflect how violent extremist groups on the continent might operate in the future. Notably, the diffusion of skills, tactics, techniques, and procedures across terrorist groups takes place regularly and globally. From al-Qaeda to Da'esh, from European neo-Nazi organizations to emergent racist and xenophobic actors in Southeast Asia, and from hybrid criminal networks like Com (764 and 09A, in particular) to a wide range of terrorist networks, terrorist actors learn from each other both inside and across ideological categories. As such, the scenarios below are designed to be relevant to praxis – not merely thought experiments.

Scenario One: Creating New Video Games and Modifications

Background: Terrorist and violent extremist actors have been creating video games for over 30 years (since 1982).⁴⁶ From standalone titles of varying sophistication to modifications (mods) for popular mainstream games, video games have been built by groups ranging from Islamic State in Iraq and the Levant (ISIL, hereinafter referred to as “Da’esh”) to neo-Nazis and racist and xenophobic identitarian groups. They are used to propagandize, to reinforce the ideological views of those playing them, to invent worlds idealized by extremists such as worlds where there is only one race, and to fundraise via game sales.

Scenario: A regional terrorist or NSAG group in the Sahel, inspired by national state-backed gaming strategies, develops custom game mods for popular first-person shooter (FPS) titles like Arma 3, as well as experiences for Roblox (the third highest-grossing game on the continent) integrating ideological narratives into mission-based gameplay. The group may also provide an Android-based short game for download via a custom .APK file hosted outside of Google Play and instead shared via third-party

⁴⁶ Emily Thompson and Galen Lamphere-Englund, *30 Years of Trends in Terrorist and Extremist Games* (Extremism and Gaming Research Network (EGRN) and the Global Network on Extremism and Technology (GNET), 2024), <https://gnet-reports.com/30-years-terrorist-extremist-games>.



file sharing sites, Telegram groups, or off-market app stores. It would likely be named innocuously to appeal to their target audience while avoiding immediate association with the organization, in order to circumvent content take-downs.

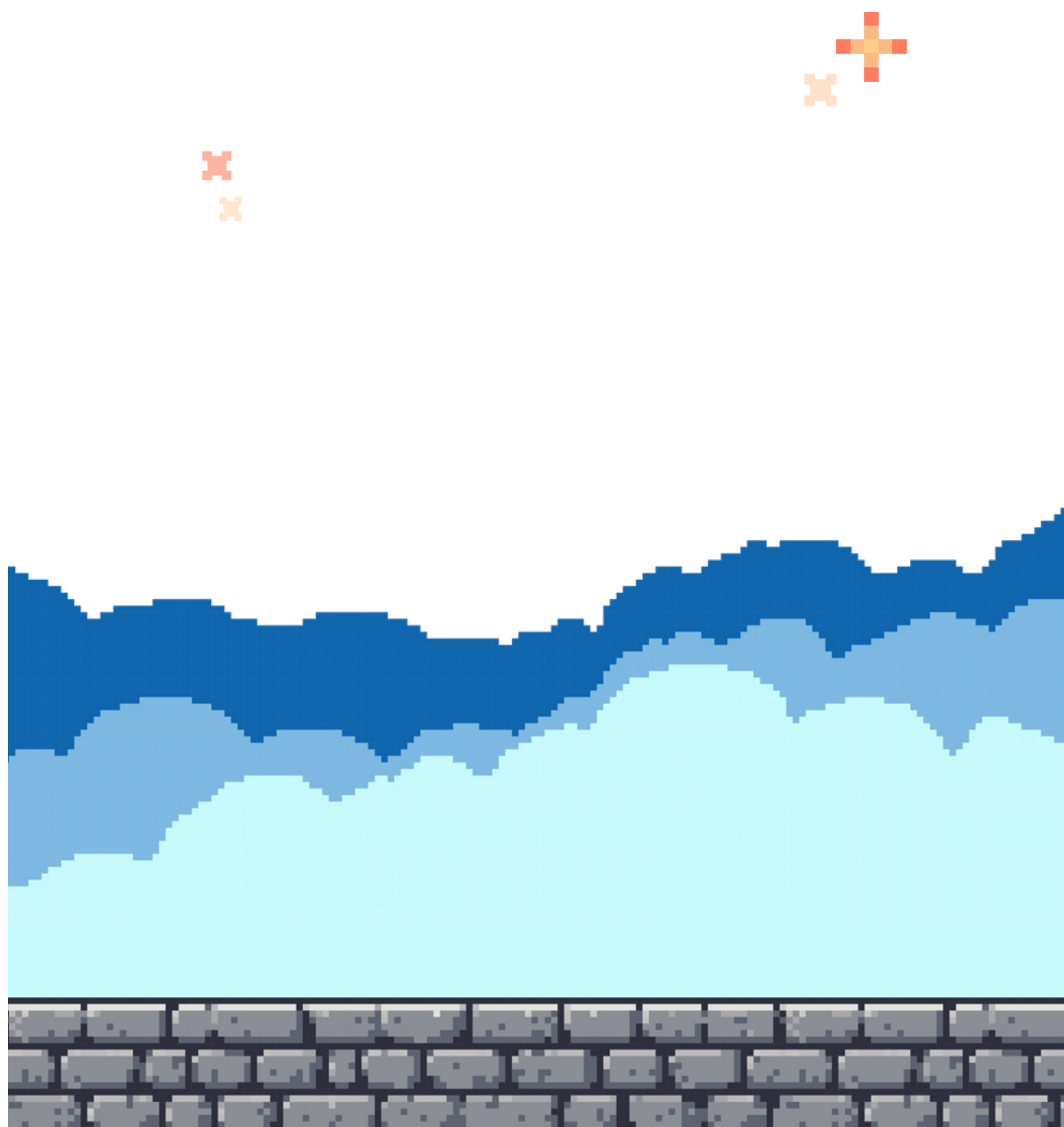
Potential perpetrators: Jama'at Nasr al-Islam wal-Muslimin (JNIM) or an affiliate disseminates terrorist content through the Az-Zallaqa foundation. JNIM is known to exploit online financing mechanisms and directly uses social media platforms for recruitment to violence and communication across Mali and elsewhere⁴⁷. Jumping to games – as their target recruitment audiences play more of them – is a sensible propaganda trajectory.

Techniques Potentially Used:

- ✖ **Localized experiences, especially built for games where players can create their own experiences (so-called sandbox games) like Roblox or Minecraft, and potentially bespoke mobile games** designed to recruit and radicalize young players to violence in conflict zones where JNIM operates (e.g., Mali, Burkina Faso, Niger). Niger stands out as a probable location given the rapid increase in gaming markets there.
- ✖ **Narrative-driven modifications for First Person Shooter (FPS) games** that depict violent extremists and terrorists as liberators fighting so called “Western Imperialism” or local government forces.
- ✖ **Games distributed through gaming communities** on Discord, Telegram, Steam, and on local pages on mainstream social media platforms, such as Facebook, Instagram, and TikTok. Discord is rapidly growing on the continent, including in the Sahel, and could become a logical dissemination point for meeting and sharing violent extremist content.
- ✖ **Gamified “combat training” missions recreating real-world JNIM battles** that blur the line between virtual play and real-world violent action. These may also be integrated into the custom games and mods. For example, Al-Qaida trained for the 9/11 attacks with Microsoft Flight Simulator games which, while dated, represents a real-world case study of gaming being used for combat training by a terrorist group.

⁴⁷ Az-Zallaqa Foundation, “Az-Zallaqa Foundation,” *Wikipedia*, accessed March 7, 2025, https://en.wikipedia.org/wiki/Az-Zallaqa_Foundation; Elise Vermeersch, Julie Coleman, Méryl Demuyne, and Elena Dal Santo, *Social Media in Mali and Its Relation to Violent Extremism: A Youth Perspective* (The Hague: International Centre for Counter-Terrorism, March 18, 2020), <https://icct.nl/sites/default/files/import/publication/Social-Media-in-Mali-and-Its-Relation-to-Violent-Extremism-A-Youth-Perspective.pdf>; Adam Rousselle, *From Trees to Terror: JNIM's Use of Online Rosewood Sales to Fuel Expansion, Insights*, Global Network on Extremism and Technology (GNET), November 25, 2024, <https://gnet-research.org/2024/11/25/from-trees-to-terror-jnims-use-of-online-rosewood-sales-to-fuel-expansion/>.

Risk Projection: Medium-Low. Given that terrorist and violent extremist actors are already using games and mods in settings where much of their target audience is active, the impact – helping radicalize to violence and recruit new generations of young, ideologically motivated members inspired to fight – will increase with digitization. Meanwhile, the vulnerability is substantial, given the lack of regulation at the government level and of localized trust and safety measures at the platform level.



Scenario Two: Exploiting Offline Gaming Social Environments

Background: Terrorist and violent extremist actors regularly exploit different types of toxic norms present in many gaming sub-communities. Recent work from an EGRN research consortium led by Royal United Services Institute (RUSI) found that toxicity and extremism are normalized within gaming settings, “with 30.3% (35.6% of males/24.9% of females) viewing toxicity as normalized, and 22.5% (25.1% of males/20% of females) seeing extremism as normalized.”⁴⁸ Targeted hate and harassment based on gender, ethnicity, race, sexual orientation, and religion are also common. Those toxic cultural norms have been shown to reduce overall resilience against violent extremism and increase the propensity to engage in targeted hate, which in turn creates an easy vector for recruiter targeting.

While there is less research on offline gaming spaces – like the gaming corners found across the continent – widespread documentation of harassment and misogyny in esports leagues suggests a strong parallel.⁴⁹

Scenario: Al-Shabaab leverages clandestine use of urban gaming cafés in Somalia and Kenya and carries out conversations at matatu (transit bus) stops with gamers playing popular titles like PUBG and Call of Duty on their phones to initiate recruitment interactions with young players. Al-Shabaab maintains active accounts on social media platforms and is known to develop high-quality communication via the Al-Kataib Media Foundation, radio stations, online news sources presented as legitimate outlets, and social media, especially Telegram, Facebook, OK.ru, TikTok, X, and YouTube.⁵⁰ The group is known to rapidly adapt coordinated information-sharing while integrating a wide network of offline communication agents who could be leveraged for gaming-centred recruitment.

In this scenario, games help form social bonds that recruiters seek to exploit. Gaming is known to facilitate the formation of powerful social bonds – including in the offline environments frequented mainly by young men and boys, which are ripe for targeting across the continent.

Techniques Potentially Used:

- ✘ **Terrorist recruiters working as gaming café employees** or joining gaming corner sessions might use the social bonds created through games, or the misogynistic ecosystems around them, to groom young male recruits.
- ✘ **Tournaments or “VIP game nights”** could be hosted by violent extremist recruiters offering

⁴⁸ Jessica White, Claudia Wallner, Galen Lamphere-Englund, Love Frankie, Rachel Kowert, Linda Schlegel, Ashton Kingdon, Alexandra Phelan, Alex Newhouse, Gonzalo Saiz Erasquin, and Petra Regeni, *Radicalisation through Gaming: The Role of Gendered Social Identity* (London: Royal United Services Institute (RUSI), 2024).

⁴⁹ Megan Condis, *Gaming Masculinity: Trolls, Fake Geeks, and the Gendered Battle for Online Culture* (Iowa City: University of Iowa Press, 2018).

⁵⁰ Georgia Gilroy, “The Online Frontline: Decoding al-Shabaab’s Social Media Strategy,” *CTC Sentinel* 17, no. 1 (January 2024): 25.

free play sessions for youth. This tactic has previously been used by groups in the United States and Western Europe.

- ✘ **Targeting mobile gaming players in public environments**, such as matatu stands, transit hubs, or cafés, using games played in common as an initial way to break the ice. The recruiter might then add the target via an in-game friend request, allowing them to continue building a relationship online – and offline (YEPP FGD, 2024).
- ✘ **Using gaming lingo and team-based FPS culture** to slowly radicalize frequent players to violence in a trusted, hybrid offline-online setting. Initial contacts from gaming corners or on-the-street recruitment can be quickly followed up with online matches, which can help build trust. That trust can then direct targets to more private chats – on Discord or Telegram to start – gradually indoctrinating the user with terrorist content. Over the longer term, the recruiter might bring the target into more violent extreme user groups, ask them to prove their loyalty via small tasks, and isolate them from their initial friend group while offering them incentives to join Al-Shabaab-linked groups.

Risk Projection: High. These real-world recruitment nexuses with gaming could serve as entry points for transitioning players from casual gaming to violent extremist networks. These threats could already be occurring, despite insufficient evidence to confirm this. There are no practical barriers to prevent Al-Shabaab or other well-equipped groups from using such recruitment vectors, demonstrating clear vulnerabilities. As such, this should be viewed as an imminent risk.

Scenario Three: Recruiting and Communicating in Games

Background: Terrorist and violent extremist actors are known to target users via in-game chats and adjacent platforms, taking advantage of poorly moderated voice chats and gaming text platforms. The linguistic diversity on the continent complicates platform trust and safety efforts: even widely spoken languages like Amharic are used to evade hate speech detection on platforms due to a lack of investment by platforms in moderation tools for the continent's languages.⁵¹ A recent survey across gaming platforms found that one-third (33.9%) of gamers in a seven-country study "encountered images, videos or symbols promoting extremism, while 38.2% saw endorsements of violence against specific social groups. Fully a quarter (24.9%) encountered content suggesting they join extremist groups, with younger respondents (27.7%, ages 18–28) more frequently targeted than older ones (22.2%, ages 29–44)."⁵² Gaming chat-based recruitment has also been used by groups in Europe and the United States, as well

51 Institute for Strategic Dialogue, "Hidden Hate: How Amharic Is Being Used to Evade Hate Speech Detection on TikTok," *Digital Dispatches*, March 4, 2025, https://www.isdglobal.org/digital_dispatches/hidden-hate-how-amharic-is-being-used-to-evade-hate-speech-detection-on-tiktok/.

52 White et al., *Radicalisation through Gaming: The Role of Gendered Social Identity* (London: Royal United Services Institute (RUSI), 2024).

as in Indonesia, where members of the security services have been targeted via FPS game chats.⁵³ Individuals in Germany have also been radicalized to violence after initially joining hate-based communities through gaming affinity groups.⁵⁴

Scenario: Recruiters affiliated with Islamic State in West Africa Province (ISWAP) factions, or JNIM and constituent member organizations such as Al-Qaeda in the Islamic Maghreb (AQIM) begin covertly targeting and communicating with new members using in-game voice chat in PUBG Mobile, Free Fire, and Call of Duty Mobile, avoiding detection by security agencies. ISWAP operates widely across the Lake Chad Basin region, including in Nigeria, Niger, Chad, and Cameroon, while AQIM is present across the wider Sahel, including in Mali, Niger, and Algeria. Mobile game chat targeting could form a first approach for recruiters targeting young men in urban or peri-urban settings more likely to have Internet connectivity and smartphone access.

Techniques Potentially Used:

- ✗ **“First-contact grooming” in mobile gaming** enables recruiters to play in public servers filtered by local languages or country tags, befriend potential recruits through casual in-game interactions, and then move them onto encrypted messaging apps such as Telegram and Signal.
- ✗ **First contacts may involve** identifying users with similar linguistic backgrounds to their target audiences, who might also respond to targeted humour based on local grievances.
- ✗ **Adding targets as friends, they may then strike up friendships** to groom the targets into joining them in other, off-game forums from Discord to encrypted Telegram, RocketChat, or Signal groups.
- ✗ **Private custom game rooms**, servers on Discord, or invite-only channels on Telegram may serve as spaces to initiate recruit vetting before directing them to terrorist and violent extremist forums or offline contacts in-country.

Risk Projection: Medium-High. These are vulnerable surfaces, as limited moderation tooling in mobile gaming is further hampered by a general lack of attention to dialects and languages spoken across the continent. Unmoderated spaces allow easy opportunities to approach, groom, and recruit users with documented implications. The anonymity afforded by most multiplayer games on mobile phones makes them an easy entry point for first contact, with recruiters operating undetected in seemingly harmless multiplayer settings.

53 Global Project Against Hate and Extremism, “How the Far-Right Spreads Hate Through Gaming,” Global Project Against Hate and Extremism, January 31, 2024, <https://globalextremism.org/post/how-the-far-right-spreads-hate-through-gaming/>.

54 Daniel Koehler, Verena Fiebig, and Irina Jugl, “From Gaming to Hating: Extreme-Right Ideological Indoctrination and Mobilization for Violence of Children on Online Gaming Platforms,” *Political Psychology* 43, no. 6 (2022): 12812, <https://onlinelibrary.wiley.com/doi/full/10.1111/pops.12812>.

There is a balance to be struck between protecting human rights and freedom of expression – without veering into censorship – and ensuring the safety of players. Because these spaces remain vulnerable, the potential impact is high. However, with groups like ISWAP and AQIM readily recruiting from their existing offline networks, expansion into gaming-based recruitment is less likely unless specific targeting of urban youth is of interest to achieve tactical objectives, such as attacks in capital cities. There are no structural barriers at present for terrorist groups to begin implementing this exploit, and the cost for recruiters is low – limited mainly to smartphones, anonymized accounts, and VPN access. This means the risk is imminent and the timeline to implementation negligible in the event of an adversarial shift. Given that the vulnerability is clear, the risk posed by this exploit is medium-high and should be monitored immediately in areas known to be targeted by terrorist actors.

Scenario Four: Gamifying Terrorist Content

Background: Terrorists actively appropriate game-like elements into non-game settings to improve engagement with their content. From leaderboards and point systems ranking xenophobic terrorist perpetrators, to live-streaming of attacks on video platforms popular with gamers, gamification is trending among terrorist groups because it is effective.⁵⁵ Helmet camera footage from perpetrators mirrors gameplay from first-person shooters, particularly Let's Play videos created by gaming influencers, immersing and inspiring viewers to recreate attacks. So-called “easter eggs” (hidden visual references), or small clues buried in the content, are also given to increase audience retention. No fewer than seven attacks, including and inspired by the 2019 Christchurch, New Zealand, massacre have sought to use livestreaming, while additional attacks appear to have drawn inspiration from livestreams, with the perpetrator of the 2022 anti-LGBT+ attack in Bratislava in Slovakia noting that the Christchurch attacker's video was “genuinely unique – maybe it was the fact that it was livestreamed, or the video-game-like view of the whole event... The video felt ‘different’ to most other content I had seen before.”⁵⁶ During the initial livestream, content is typically rapidly backed up by viewers and outlinked to video and file-sharing sites, making later take-downs extremely challenging. Twitch, for example, reacted within two minutes to the livestream of the attack in Buffalo, NY, USA in 2022. Still, the initial viewers recorded and re-shared the content, which has since been viewed hundreds of thousands of times.⁵⁷ Gamification can include various elements beyond livestreaming, from the aforementioned scoreboards where sympathizers give points for the number of civilians killed by perpetrators, to adapting avatars in games to look like terrorists.

55 Suraj Lakhani and Susann Wiedlitzka, “Press F to Pay Respects: An Empirical Exploration of the Mechanics of Gamification in Relation to the Christchurch Attack,” *Terrorism and Political Violence*, 2022, <https://www.tandfonline.com/doi/full/10.1080/09546553.2022.2047589>.

56 Petra Regeni, *Accelerationism Meets Gamification: A Look at the Convergence in the Framing of Online Narratives*, GNET Insight, Global Network on Extremism and Technology (GNET), May 31, 2023, <https://gnet-research.org/2023/05/31/accelerationism-meets-gamification-a-look-at-the-convergence-in-the-framing-of-narratives-online/>.

57 Galen Lamphere-Englund and Jessica White, “The Buffalo Attack and the Gamification of Violence,” *Royal United Services Institute (RUSI)*, May 16, 2022, <https://www.rusi.org/explore-our-research/publications/commentary/buffalo-attack-and-gamification-violence>.

Location	Date	Fatalities/ Injuries	Manifesto posted on	Livestream	Outlinking
Christchurch, New Zealand	15Mar-19	51 fatalities	8chan, /pol/	Facebook	File-sharing sites (self)
Poway, USA	27-Apr-19	1 fatality	8chan, /pol/	Facebook (attempted)	(Unknown)
Bærum, Norway	10-Aug-19	1 fatality	Endchan	Facebook (attempted)	(Unknown)
Halle, Germany	9-Oct-19	2 fatalities	Meguca	Twitch	(Unknown)
Buffalo, USA	14-May-22	10 fatalities	Discord, Google Docs	Twitch	File-sharing sites by supporters, Kiwifarms
Eskişehir, Turkey	12-Aug-24	5 injured	Telegram	Kick	Telegram, Mediafire
Antioch, USA	22-Jan-25	2 fatalities	X	Kick	Kiwi Farms, X

Offline Attacks with Gamified or Livestreaming Elements. Adapted and extended from Thorleifsson, 2021, p. 7.⁵⁸

Scenario: Boko Haram and similar groups step up livestreaming and gamification of attacks by integrating real-life attack livestreams and gamified challenges on gaming-adjacent platforms such as Twitch, Trovo, Kick, and DLive. The group is already known to exploit video content of their attacks for propaganda purposes, such as footage filmed during the 2014 Giwa Barracks attack in Maiduguri, Nigeria.⁵⁹ Similarly, Al-Shabaab live-tweeted during the deadly assault on Westgate Mall in Nairobi, Kenya, in 2013, setting a precedent for using technology to amplify the spectacle of terror in real-time.⁶⁰ Despite an improved overall security situation, Boko Haram remains active in 2025 in North East Nigeria and surrounding regions. Coupled with improving infrastructure access, the possibility of the group livestreaming attacks in real-time – with gamified elements such as helmet-camera footage and “easter eggs” for viewers – is highly plausible. Limited oversight on platforms like Kick and DLive, or platforms popular with Arabic-speaking audiences like Trovo, may mean that such attack videos are not quickly removed, increasing engagement.

58 Thorleifsson, C., & Düker, J. (2021). “Lone Actors in Digital Environments,” Radicalisation Awareness Network (RAN). https://home-affairs.ec.europa.eu/system/files/2021-10/ran_paper_lone_actors_in_digital_environments_en.pdf.

59 Ameh Comrade Godwin, “Boko Haram Releases Video of Attack on Giwa Barracks [WATCH],” *Daily Post Nigeria*, March 28, 2014, <https://dailypost.ng/2014/03/28/boko-haram-releases-video-attack-giwa-barracks-watch/>; Amnesty International, “Nigeria: Gruesome Footage Implicates Military in War Crimes,” August 5, 2014, <https://www.amnesty.org/en/latest/news/2014/08/nigeria-gruesome-footage-implicates-military-war-crimes/>.

60 Victoria Fassrainer, “Tweeting Terror Live,” Army University Press, March-April 2020.

Techniques Potentially Used:

- ✘ **Attack “scoreboards”** on Telegram or end-to-end encrypted (E2EE) platforms that reward supporters who predict or “vote” on targets before attacks. Potentially target selection becomes gamified, with the most popular targets being selected for kinetic operations.
- ✘ **Live combat feeds framed as “real-life FPS matches,”** with commentary mirroring eSports tournaments, are used to propagate attacks, intimidate adversaries, and reach younger audiences used to video game feeds.
- ✘ **Custom gamified apps for connecting recruits or like-minded individuals,** mirroring Pokemon Go similarly to the Patriot Peer app developed by racist and xenophobic groups in Germany to connect followers in the same geographic areas.
- ✘ **Leaderboard rankings for fighters** encourage competition among youth radicalized to violence to carry out higher-profile attacks or step up their ‘kill counts’ in real-world scenarios.
- ✘ **Recreations of attacks in games for training purposes.** Boko Haram already uses offline training games for young recruits and child soldiers. The group works to desensitize children to violence, build social cohesion, and prepare them for combat.⁶¹ In the future, the group may use recreations drawn from videos of attacks to duplicate the incidents in games – or even in virtual reality (VR) – for training purposes. Racist and xenophobic attackers have also recreated atrocities to radicalize others to violence and train recruits. It is notable that nation-state militaries already use games and VR to train their troops.

Risk Projection: High. Adopting the livestreaming of terrorist attacks, at least in some instances, will likely occur as Internet infrastructure increasingly allow it. This is more likely to happen, not in frontline or remote locations, but rather through surprise attacks carried out in urban areas or locations without restricted Internet access. There is a well-documented transference of successful tactics, techniques, and procedures from racist and xenophobic to violent groups aligned with or inspired by Da’esh. This threat may well make its way to the continent soon. Furthermore, normalizing real-world violence as an extension of gaming may lower psychological barriers to participating in terrorist acts or joining terrorist groups, increasing the potential impact. While distinct from the threat posed by recruitment and radicalization to violent approaches, there is a similarly low barrier to entry for terrorist groups and a potentially high reward from increased engagement with attack propaganda. In areas with persistent Internet access, sufficient bandwidth, and active violent extremist groups, there is an imminent and increasing risk of this tactic being adopted.

⁶¹ Amnesty International. (2015). Nigeria: Crimes under international law committed by Boko Haram and the Nigerian military in north-east Nigeria: Amnesty International. Statement to the 29th session of the UN Human Rights Council (15 June – 3 July 2015).

AFR 44/1756/2015. <https://www.amnesty.org/en/wp-content/uploads/2021/05/AFR4417562015ENGLISH.pdf>; Bloom, M., & Warpinski, K. K. (2021, March 25). Children in violent movements: From child soldiers to terrorist groups. Oxford Research Encyclopedia of International Studies. <https://doi.org/10.1093/acrefore/9780190846626.013.602>.

Scenario Five: Using Gaming References and Aesthetics for Propaganda

Background: As illustrated above, games are salient pop culture references for an increasingly large group of African gamers. Global trends in violent extremist uses of games for propaganda show that they are employed not only as gaming experiences, but also as references in other content, providing still graphics, memes, and videos for violent extremist groups to disseminate.⁶² From Da'esh using Grand Theft Auto IV in recruitment videos, to neo-Nazi groups drawing on Far Cry V for meme content, gaming references make powerful, salient propaganda.⁶³ The rise of User-Generated-Content (UGC) and experiences, from sandbox games that create entire worlds to simple player avatars and skins (outfits for in-game characters) inside games like Fortnite and Minecraft, also allows for gamified propaganda to be easily created within existing games. That content may be meant for consumption inside servers, such as Da'esh training camps made in Singapore and Nazi internment camps for German audiences, or for distribution of images outside, such as clips from Assassin's Creed Valhalla used by racist and xenophobic groups in northern Europe.⁶⁴ Meanwhile, generative artificial intelligence (AI) image-diffusion tools make it easy for violent extremist groups to create game- and anime-like content with violent extremist overtones.⁶⁵

Scenario: Al-Shabaab or JNIM creates propaganda designed to look like anime or other comic formats using Minecraft and Roblox experiences and disseminating it via social media through short videos crafting visually appealing, memeified radicalization to violence content targeted at young players. These have the added advantage of often evading content moderation if carefully crafted. As discussed previously, Al-Shabaab uses a wide range of technology-amplified recruitment approaches. Other groups could readily adopt the approach as well, such as the Lakurawa, recently designated a terrorist organization by

Nigeria, and known to use social media for recruitment and drones to monitor their military opposition.⁶⁶

62 Ashton Kingdon, *God of Race War: The Utilisation of Viking-Themed Video Games in Far-Right Propaganda*, GNET Insight, Global Network on Extremism and Technology (GNET), February 6, 2023, <https://gnet-research.org/2023/02/06/god-of-race-war-the-utilisation-of-viking-themed-video-games-in-far-right-propaganda/>; Ashton Kingdon, "Beauty is Power: The Use of Gaming References and Gaming Aesthetics in Extremist Propaganda," in *Gaming and Extremism: The Radicalization of Digital Playgrounds*, eds. Linda Schlegel and Rachel Kowert (New York: Routledge, 2024), <https://doi.org/10.4324/9781003388371>.

63 Miron Lakomy, "Let's Play a Video Game: Jihadi Propaganda in the World of Electronic Entertainment," *Studies in Conflict & Terrorism*, vol. 41, no. 5 (May 2018): 383–406, <https://doi.org/10.1080/1057610X.2017.1385903>; Firas Mahmoud, *The Gamification of Jihad: Playing with Religion* (Copenhagen: Danish Institute for International Studies, 2021), <https://research.diis.dk/en/publications/the-gamification-of-jihad-playing-with-religion>; Cori E. Dauber, Mark D. Robinson, Jovan J. Baslious, and Austin G. Blair, "Call of Duty: Jihad – How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos," *International Centre for Counter-Terrorism*, vol. XIII, no. 3 (April 11, 2023), <https://pt.icct.nl/article/call-duty-jihad-how-video-game-motif-has-migrated-downstream-islamic-state-propaganda>.

64 Mariana Olaizola Rosenblat, *Gaming the System: How Extremists Exploit Gaming Sites and What Can Be Done to Counter Them* (New York: NYU Stern Center for Business and Human Rights, 2023), <https://bhr.stern.nyu.edu/tech-gaming-report>.

65 Louis Dean, *AI or Aryan Ideals? Part Two: A Thematic Content Analysis of White Supremacist Engagement with Generative AI Discourse*, GNET Insight, Global Network on Extremism and Technology (GNET), February 25, 2025, <https://gnet-research.org/2025/02/25/ai-or-aryan-ideals-part-two-a-thematic-content-analysis-of-white-supremacist-engagement-with-generative-ai-discourse/>.

66 "DHQ Confirms Lakurawa Terrorists Use Social Media, Money to Recruit Nigerian Youths," *Ripples Nigeria*, November 13, 2024, <https://www.ripplesnigeria.com/dhq-confirms-lakurawa-terrorists-use-social-media-money-to-recruit-nigerian-youths/>; "Lakurawa Terror Group Using Drones To Track Military, Civilians – Experts," *The News Desk*, November 12, 2024, <https://thenewsdesk.ng/2024/11/12/lakurawa-terror-group-using-drones-to-track-military-civilians-experts/>.



Gendered differences in online recruitment would be worth assessing in future studies, as Al-Shabaab has been known to use female recruits for fundraising, exploiting gendered stereotypes to circumvent financial transfer oversight.

Notably, this scenario blurs into the creation of games and mods. Yet it differs from Scenario One in that the threat actor intends to use easy-to-create user-generated content for further dissemination, not for the gameplay itself.

Techniques Potentially Used:

- ✖ **Minecraft “rebuilt” of violent extremist-occupied territories** as user-generated content, with the in-game experiences framing them as “liberated” zones to attract young sympathizers.
- ✖ **Roblox-based violent extremist mini-games** designed to glorify past terrorist operations while presenting them as heroic struggles. These would likely be subtly coded and named to avoid immediate detection by content-moderation algorithms. They may also be created in Somali and Arabic.
- ✖ **Images and short videos mirroring the gameplay style and graphics created for memes** and designed to be shared across social media. Potentially generative AI tools could also be used for this.
- ✖ **Disseminating violent extremist gameplay clips on TikTok, YouTube Shorts, and Instagram Reels and in Telegram groups** to circulate propaganda.
- ✖ **Gameplay sharing overlaid with recruitment memes and text on Facebook and Telegram** to amplify the violent extremist content further.

Risk Projection: High. The immediate impact of gamified violent extremist content is increased visibility among younger gamers, a core target demographic for many terrorist groups. As such, one could see threat actors like Al-Shabaab developing an approach like the above in Kenya and parts of Somalia. Other groups with territorial holdings, such as JNIM, which continues to blockade towns in Mali,⁶⁷ may develop similar approaches. In doing so, terrorist groups help facilitate radicalization by turning terrorist iconography and landmarks into viral, easily consumable gaming content. As with other scenarios discussed here, the barrier to entry is low, with substantial vulnerabilities, and the potential upsides are significant, especially in areas with larger gaming communities. As such, the risk is high.

67 Africa Defense Forum, “JNIM Militants Continue Blockade of Malian Towns,” *ADF Magazine*, January 2025, <https://adf-magazine.com/2025/01/jnim-militants-continue-blockade-of-malian-towns/>.



Scenario Six: Financing of Terrorism and Money Laundering

Background: The prospect of terrorist groups using gaming for financing and money laundering has been raised by experts for at least five years, but limited evidence has surfaced of specific instances.⁶⁸ In general, terrorist groups have little need to resort to gaming-based financing when other, easier options are still accessible. However, the sale of actual games has been used by groups as a means to raise funds for their organizations.⁶⁹ Meanwhile, crypto contributions from DLive, a livestreaming platform popular with gamers, have been used to fund groups in Germany.⁷⁰ Further risks are present: money laundering through gaming platforms using third-party markets to sell in-game items and game keys; in-game currency accumulation and resale; and gambling through sandbox games used as secondary marketplaces.⁷¹ A recent analysis of the sales related to the popular game CS:GO on Steam found that illicit financing was likely taking place and could be detected by researchers.⁷² Meanwhile, a recent Financial Action Task Force (FATF) report found that Al-Shabaab is “reported to have abused an online gambling platform registered in the Caribbean for [terrorist financing] TF,” while prior accounts in South Africa linked to terrorist activity in Somalia and Da’esh were found to have been making transfers to the PlayStation Network online.⁷³

Scenario: Terrorist and affiliated criminal networks in Somalia use in-game microtransactions and mobile game economies to launder money through popular multiplayer games with tradeable assets. Somali officials are actively working to clamp down on the US\$100 million in estimated revenues a year that Al-Shabaab brings in via “complex web of crimes, including extorting shippers at the country’s ports, posting checkpoints on major roads, blocking roads to force travellers to travel through al-Shabaab-controlled communities, and forcing businesses and citizens under its influence to pay [a 2.5% tax].”⁷⁴ With increased state capacity and counter terrorism financing efforts, including the arrests of 37 individuals across East Africa suspected of supporting Al-Shabaab and Da’esh in 2024,⁷⁵ the group may well look for additional options to launder its assets through digital means. The most recent report to the United

68 Moshe Klein, “Video Games Might Matter for Terrorist Financing,” *Lawfare*, May 30, 2024, <https://www.lawfaremedia.org/article/video-games-might-matter-for-terrorist-financing>.

69 Emily Thompson and Galen Lamphere-Englund, “30 Years of Trends in Terrorist and Extremist Games,” *GNET and Extremism and Gaming Research Network*, November 2024, 29–30, https://gnet-research.org/wp-content/uploads/2024/10/GNET-47-Extremist-Games_web.pdf.

70 “Jeder wirbt für sich allein? Wie auf Telegram der Aufruhr zum Geschäft wird,” *Machine Against the Rage*, accessed March 10, 2025, <https://machine-vs-rage.bag-gegen-hass.net/jeder-wirbt-fur-sich-allein/https://machine-vs-rage.bag-gegen-hass.net/jeder-wirbt-fur-sich-allein/>.

71 “Digital Technology and Money Laundering,” *ABC News*, July 21, 2024, <https://www.abc.net.au/news/2024-07-21/digital-technology-and-money-laundering/104081836>.

72 Dan Cooke and Angus Marshall, “Money Laundering Through Video Games: A Criminals’ Playground,” *Forensic Science International: Digital Investigation* 50 (2024): 301264, <https://doi.org/10.1016/j.fsidi.2024.301264>.

73 Financial Action Task Force, Comprehensive Update on Terrorist Financing Risks (Paris: FATF-OECD, July 8, 2025). <https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.pdf.coredownload.inline.pdf>.

74 Africa Defense Forum, “Somalia Puts Financial Squeeze on al-Shabaab,” *ADF Magazine*, March 2025, <https://adf-magazine.com/2025/03/somalia-puts-financial-squeeze-on-al-shabaab/>.

75 “37 Terror Suspects Arrested in East African Operation,” *INTERPOL*, January 27, 2025, <https://www.interpol.int/en/News-and-Events/News/2025/37-terror-suspects-arrested-in-East-African-operation>.

Nations Security Council by the Analytical Support and Sanctions Monitoring Team established pursuant to resolutions 1526 (2004) and 2253 (2015) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities.⁷⁶

In particular, in this scenario, Al-Shabaab and affiliated entities, or other groups across the continent, could use a combination of CS:GO in-game item betting (a format of gambling), game key laundering, and cryptocurrency outflow schemes to move funds across the region with relative impunity in the face of heightened enforcement across typical financing networks. In doing so, they would take advantage of regulatory gaps surrounding gaming and microtransactions in general – and particularly on the continent.

✖ Techniques Used:

- ✖ **“Skin gambling” and micro-transactions sold through third-party marketplaces** in games like Call of Duty Mobile, Lords Mobile, and Free Fire are used to transfer money between fake accounts trading in-game assets. This may be particularly lucrative across smaller games with fewer Know Your Customer (KYC) protocols.
- ✖ **Overpriced game sales through Steam** can be used to create game keys that are saleable on third party platforms like Kinguin. This may entail using recruited and (poorly) paid individuals, to purchase the games and resell them at high volumes without significant profit loss, though Steam-based networks may incur up to 45% in laundering costs.⁷⁷
- ✖ **Using African fintech services, such as mobile money and new crypto exchanges, to obscure financial trails** while routing funds through in-game economies. By using mobile money to buy in-game items, then cashing out via a sale to a fake account, owned by the same user, on the leading game platform or a third-party marketplace that supports cryptocurrencies, the launderer can readily transfer funds via gaming platforms to a clean crypto wallet not monitored by security services.
- ✖ **Using taxation of criminal syndicates for the manipulation of gaming services to obtain funds.** While Al-Shabaab and other terrorist groups may not operate their own gaming financing operations, criminal syndicates in their areas of operation (especially in Somalia) are subject to taxation by the terrorist groups. This may result in the event of criminal groups seeking to manipulate gaming services and indirect financial gains for violent extremist groups.

76 United Nations Security Council, “Thirty-Fifth Report of the Analytical Support and Sanctions Monitoring Team Submitted Pursuant to Resolution 2734 (2024) Concerning ISIL (Da'esh), Al-Qaida and Associated Individuals and Entities,” *United Nations Security Council*, February 6, 2025, https://digitallibrary.un.org/record/4076001/files/S_2025_71_Rev.1-EN.pdf.

77 For examples: Upper Echelon, *The Dark Side of Steam - Laundering Money*, YouTube video, 17:42, October 9, 2021, https://www.youtube.com/watch?v=BFmBT_Avf48; Progress, *How to Launder Money on Steam*, YouTube video, 12:18, May 15, 2023, <https://www.youtube.com/watch?v=qcoVNJcrz2o>.

Risk Projection: Low. Gaming's lack of financial oversight in microtransactions makes it a potentially lucrative tool for laundering money without detection when other means are closed off. However, there is little evidence to suggest that terrorist groups are actively exploiting gaming platforms at scale for financial purposes worldwide. The threat has not reached a substantial level. Given that other, traditional "methods of fundraising such as kidnapping for ransom, extortion, taxation of local communities, exploitation of natural resources and theft constituted significant portions of Da'esh revenues,"⁷⁸ along with zakat in Somalia for Al-Shabaab, and cattle rustling in the Lake Chad Basin by Boko Haram, the likelihood of using gaming services for financing and money laundering on the continent is relatively low. Overall, while the vulnerability exists, the threat is not yet present, and the overall impact is not significant. The risk, thus, is low.

Scenario Takeaways:

These six scenarios present a realistic but speculative threat model based on known global terrorist and violent extremist gaming exploits adapted to the African context. They illustrate how offline and online gaming spaces can converge, creating new recruitment pipelines, financial networks, and propaganda tools for violent extremists and terrorist groups. As we have seen:

1. CREATING NEW VIDEO GAMES AND MODIFICATIONS

Risk Projection: Medium-Low.

Groups like JNIM, Da'esh, Al-Shabaab, and others present on the continent, like Allied Democratic Forces (ADF), could soon develop localized game modifications and mobile games to reinforce their narratives, mimicking strategies already seen in violent extremist movements worldwide.

2. EXPLOITING OFFLINE GAMING SOCIAL ENVIRONMENTS

Risk Projection: High.

Offline and online recruitment pipelines – outlined in scenarios Two and Three - are converging, with gaming cafés, mobile multiplayer interactions, and in-game chat functions becoming vectors for radicalization to violence.

3. RECRUITING AND COMMUNICATING IN GAMES

Risk Projection: Medium-High.

Meanwhile, Boko Haram and other actors may begin livestreaming attacks, gamifying real-world violence much like racist and xenophobic attackers have done.

⁷⁸ United Nations Security Council, "Thirty-Fifth Report of the Analytical Support and Sanctions Monitoring Team Submitted Pursuant to Resolution 2734 (2024) Concerning ISIL (Da'esh), Al-Qaida and Associated Individuals and Entities," *United Nations Security Council*, February 6, 2025.

4. GAMIFYING TERRORIST CONTENT AND USING GAMING AESTHETICS FOR PROPAGANDA

Risk Projection: High.

Violent Extremist propaganda in gaming is also evolving, with groups using Roblox and Minecraft machinima or gaming-themed meme culture to spread ideology.

5. FINANCING TERRORISM AND LAUNDERING MONEY

Risk Projection: Low.

Lastly, while traditional financing methods remain dominant, terrorist groups may exploit microtransactions, third-party gaming marketplaces, and crypto-backed game assets as financial enforcement tightens.

While the degree of risk varies across the six scenarios, clear vulnerabilities, threats, and tangible impacts on security are present. With the rapid adoption of gaming across the continent, it is time to act pre-emptively to keep games safe. Gaming companies, law enforcement, and counter-terrorism actors must act proactively, enhancing content moderation, digital financial oversight, and gaming literacy programmes to disrupt violent extremist networks before they fully take hold in Africa's rapidly expanding gaming ecosystem. Content moderation and oversight efforts should embed human rights safeguards to ensure that their implementation does not undermine fundamental rights, including the right to privacy and the rights to freedom of expression and freedom of association, as defined under international human rights law. Cooperation between public and private actors involved in these efforts is crucial to promote human rights-based approaches to content moderation and oversight.



* **PREVENTION AND RESILIENCE**

BUILDING OPPORTUNITIES *

Thankfully, gaming is increasingly being harnessed for positive impacts, particularly throughout Africa. While gaming companies, law enforcement, and P/CVE, as well as CT experts, must pre-emptively address risks through better human rights-based content moderation, digital financial oversight, and gaming literacy programmes targeting vulnerable youth, good case studies are already present across the continent.

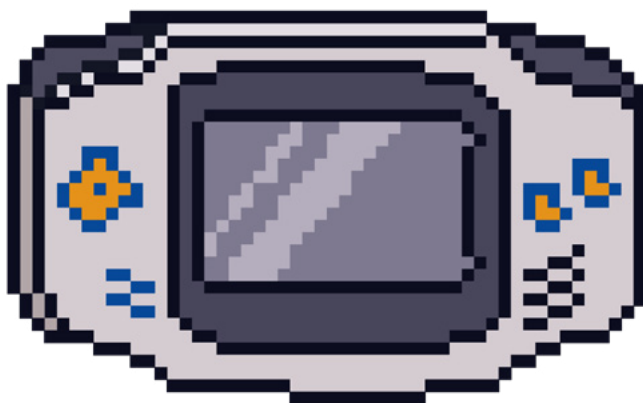
The Global Internet Forum to Counter-Terrorism (GIFCT) and the Extremism and Gaming Research Network (EGRN) recently released *Prevent, Detect, and React: A Framework for Countering Violent Extremism on Gaming Surfaces*,⁷⁹ a guidance document reflecting on over five years of good practice and provides a series of concise case studies, with clear recommendations for those seeking to secure gaming ecosystems against violent extremist exploitation. The recommendations are divided into the three main categories listed below:

1. **Prevent:**
 - ▶ Denounce Terrorist and Violent Extremist Exploitation of Gaming Platforms
 - ▶ Design Games and Gaming Experiences With User Safety in Mind
 - ▶ Improve Knowledge and Awareness of Online Harms
 - ▶ Support Communities Through Positive Interventions
2. **Detect:**
 - ▶ Train Humans (for moderation and law enforcement)
 - ▶ Train Machines (for machine-led and AI content flagging)
 - ▶ Share Signals (between governments, law enforcement, and platforms)
3. **React:**
 - ▶ Provide Easy User Reporting (of terrorist and violent extremist abuse and content)
 - ▶ Automate Reactive Player Mechanics (to automatically work on norms change)
 - ▶ Pursue Positive Post-Violation Gaming Behavioural Change Among Players
 - ▶ Make Mental Health, Psychosocial Support, and Law Enforcement Referrals

⁷⁹ Conflict of interest statement: This report was authored by the same lead author as this study and received funding from GIFCT to provide the guidance framework. Galen Lamphere-Englund, *Prevent, Detect, and React: A Framework for Countering Violent Extremism on Gaming Surfaces*, Global Internet Forum to Counter Terrorism (GIFCT), February 2025, <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-PDR-Surfaces-1.1.pdf>.



Research for this report revealed excellent examples of prevention initiatives utilizing gaming for positive impact across the continent, detailed and elaborated on below. However, detection and reaction efforts were not readily uncovered apart from platform-wide initiatives at significant gaming and social media platforms. These, as mentioned, are often not attuned to linguistic realities and threat-actor contexts across the continent. As such, there is room for improvement, as discussed in the recommendations portion of this report.



Using Gaming for Good: Case Studies

Drawing on interviews carried out for this report, along with a prior impact report from the Pan Africa Gaming Group (PAGG), several previously released games are highlighted that have contributed to raising awareness of social issues, such as online harms, along with initiatives that strengthen positive gaming communities. Only a few PCVE initiatives have been deployed in online gaming spaces: drawing inspiration from wider positive gaming initiatives on the continent helps draw analogies relevant for the field. There are a few others offline gaming-related PCVE examples from European contexts, as well as educational-entertainment games that can also fit well into PCVE work and are worth referencing.⁸⁰

Games: The use of games for PCVE requires caution, as the development of standalone games is expensive, difficult to execute effectively, and not always the best avenue to reach target audiences. Recent guidance suggests that prevention practitioners might be better served by building mods for existing games, creating sandbox experiences, and using other social gaming services, such as in-game chats, game-focused communication platforms, and livestreaming services.⁸¹ That said, a few exemplary games from the continent frame how standalone games can be built to raise awareness of social issues. Typically, such titles are best deployed in partnership with educational institutions or community outreach projects.⁸²

Wewe.vote – Strengthening Democratic Engagement

- ✖ Developed by Usiku Games in collaboration with the British Council, Google.org, and the United Nations Development Programme (UNDP), this game educates youth on peaceful democratic participation, combating misinformation, and promoting election integrity.
- ✖ The title uses humour, AI voice cloning, and interactive storytelling to engage players, focusing on reducing vote-buying and tribalism during elections.
- ✖ The web-first model provides a strong basis for reaching connected audiences when deployed alongside other voter education initiatives.

⁸⁰ See, for example, chapters on interventions in Linda Schlegel and Rachel Kowert, eds., *Gaming and Extremism: The Radicalization of Digital Playgrounds* (Routledge, 2024), <https://www.taylorfrancis.com/books/oa-edit/10.4324/9781003388371/gaming-extremism-linda-schlegel-rachel-kowert>.

⁸¹ Linda Schlegel, Jessica White, and Petra Regeni, *Implementing Positive Gaming Interventions: A Toolkit for Practitioners*, Royal United Services Institute (RUSI), 2025, <https://www.rusi.org/explore-our-research/publications/special-resources/implementing-positive-gaming-interventions-toolkit-practitioners>.

⁸² Examples include those from: Pan Africa Gaming Group (PAGG), *PAGG Impact Report 2023*, 2023.

Mission 55 – African Union Peace & Security Education

- ✖ Developed by the Pan Africa Gaming Group (PAGG) with funding from the African Union and the German Agency for International Cooperation (Deutsche Gesellschaft für Internationale Zusammenarbeit – GIZ), this Risk-style strategy game teaches players about Africa's Peace and Security Architecture (APSA).
- ✖ Players navigate conflict-resolution scenarios, learning about the role of mediation, peace-keeping, and diplomacy.
- ✖ Limited distribution and funding affected the overall reach of the title.

Electric Blue – Wildlife Conservation Through Gaming

- ✖ Developed in partnership with a charity conservation group, On The Edge, to raise awareness of Tanzania's endangered Electric Blue Gecko.
- ✖ A highly engaging mobile game that subtly educates players on conservation while keeping the gameplay fun and immersive, it is a rare example of an organically and widely played game-for-good, with over 500,000 downloads on the Google Play Store.

Communities

Cross-sectoral networks are critical to building links between the gaming industry, governments, and civil society actors. These efforts also help to build the trust necessary to tackle social harms like violent extremism. Due to fears of creating a moral panic, industry representatives are often reluctant to speak with counter-terrorism officials, making it necessary to build prior relationships grounded in mutual understanding of both the harms present and the broadly positive nature of most games.⁸³ Across Africa, social-good summits and networks related to gaming could be mirrored for violence prevention and PCVE efforts.

Networks

Pan Africa Gaming Group (PAGG)

- ✖ The Pan Africa Gaming Group (PAGG) is a collective of leading African game studios dedicated to growing the gaming industry globally. Launched at Africa Games Week 2022 in

⁸³ Galen Lamphere-Englund and Menso Hartgers, *CTRL+ALT+COLLABORATE: Public-Private Partnerships to Prevent Extremism in Gaming*, RAN Policy Support, February 2024, https://home-affairs.ec.europa.eu/document/download/e446f013-34e1-4f74-bce6-90f661937ce9_en.

Cape Town, PAGG brings together 10 game development studios and a network of 300+ game professionals across Africa, fostering co-production, knowledge sharing, and industry expansion. The group has produced games tackling democracy education (Wewe.vote), climate change (Let It Rain), and online safety (Cyber Soljas).

Game Jams and Summits

Green Games Summit

- ✖ An inaugural games-for-change summit took place in Nairobi, Kenya, in February 2024, organized by the Playing for the Planet Alliance, the United Nations Environment Programme (UNEP), and the Pan Africa Gaming Group (PAGG).
- ✖ The summit highlighted leading African game studios with environmental themes, such as Usiku Games, Internet of Elephants, Mekon (Kenya), and Sea Monster (South Africa).
- ✖ The event included a Green Game Jam, which sought to create 78 games aimed at inspiring one million real-world environmental actions.

Games for Change Africa

- ✖ Games for Change Africa is a regional chapter of the global Games for Change (G4C) initiative, dedicated to leveraging video games for social impact, education, and economic development across the continent. Established in South Africa in 2021, G4C Africa focuses on spotlighting African games. The G4C Africa Festival is an annual flagship event that brings together game developers, thought leaders, and investors to discuss and showcase how games can address societal challenges.
- ✖ The 2023 and 2024 editions were held in South Africa as part of Africa Games Week. From 2025, the summit will be hosted at Fak'ugesi, one of Africa's leading digital innovation festivals, celebrating gaming, creative technology, digital arts, and interactive media.

GameUp Africa Jam for Democracy

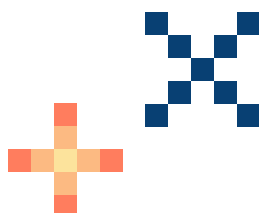
- ✖ Maliyo Games, in collaboration with the United States Consulate General in Lagos and Global Game Jam, launched the GameUp Africa Jam for Democracy to address disinformation and its impact on democratic governance. In December 2024, this initiative brought together game developers, artists, storytellers, and civic activists from Nigeria, Kenya, and Ghana to create games that explore democracy and misinformation.



Other Africa-Specific Gaming Industry Platforms⁸⁴

- ✖ **Africa Games Week (AGW):** Generally recognized as Africa's largest gaming industry event, AGW is held annually in Cape Town, South Africa, and serves as a hub for game developers, industry professionals, and investors.
- ✖ **Lagos Games Week:** Nigeria's leading gaming convention and a celebration of the country's growing gaming culture and esports scene. It serves as a key platform for building gaming communities, elevating Nigerian-made games, and connecting local talent with regional and global opportunities in the industry.
- ✖ **Africacomicade:** One of Africa's most prominent platforms for gaming, animation, and interactive media, this annual event connects African developers with global industry leaders. It also runs the SPARK and ARK Fellowships, which provide training and funding access to African game studios.
- ✖ **Playtopia:** South Africa's premier indie games and interactive arts festival, highlighting experimental games, virtual reality, and digital storytelling. Held in Cape Town, this festival celebrates alternative gaming cultures.

The willingness of many in the industry across Africa to view gaming as a positive mechanism for social change suggests strong potential for efforts to strengthen resilience against violent extremism and terrorist exploitation. The above examples of pro-social games, networks, and events provide a brief template for multi-stakeholder preventative programming that could be co-developed for PCVE and broader protection against online harms.



⁸⁴ From: Maliyo Games, 2025 *Africa Games Industry Report* (Lagos: Maliyo Games, 2025), <https://www.africagamesreport.com>.



* CONCLUSION & RECOMMENDATIONS *

The next billion gamers will be African. The continent is digitizing at a blistering pace. Yet development is unequal and not without its discontents. The most affected regions on earth by terrorism are in Africa, in particular across the Sahel. Terrorist and violent extremist actors are actively operating across much of West Africa, as well as across many countries in East Africa and the Horn of Africa. Non-state armed actors and a range of terrorist and violent extremist groups, such as the Islamic State Central Africa Province (ISCAP), are also active in Central Africa and in Mozambique, where IS Mozambique operates. From JNIM to an array of Da'esh affiliates, to Boko Haram, and Al-Shabaab, civilians and governments across at least 24 countries on the continent face regular risks of terrorism. At the same time, much of the continent lives in comparative peace: 26 countries have observed no instances of terrorism in the last five years.⁸⁵ There is little evidence of those groups using gaming surfaces to date.

However, terrorist and violent extremist actors globally are known to exploit gaming surfaces to disseminate content, radicalize to violence, recruit, and organize. This threat-modelling exercise is limited in scope: it does not draw on widespread surveys, open-source data collection, or systematic interviews with law enforcement and intelligence agencies. As such, exploitation may well be taking place already. And, if not, as audiences across the continent rapidly join the ranks of online denizens and play socially connected video games, terrorist and violent extremist actors will seek to reach their target audiences via gaming surfaces. Historically, terrorist groups are early adopters of new technologies. Groups such as JNIM, Boko Haram, and Al-Shabaab have shown a proclivity to adopt new technologies across the continent: they are likely to use gaming in the same way that Da'esh affiliates and racist and xenophobic groups have done in other contexts.

There is a rare opportunity for actors across sectors to anticipate the terrorist technology adoption curve. Counter-terrorism and PCVE practitioners are usually behind as they have been in much of the world when it comes to gaming but the context in Africa may prove to be a rare exception. Examples of gaming for good from across the continent show how games can be used impactfully to improve societies, from Kenya to Morocco to Nigeria.

The next billion gamers deserve to have their social spaces be safe, inclusive, and engaging. Now is the time to set up prevention, detection, and reaction frameworks to safeguard gaming across the continent, and especially in priority areas such as countries in the Sahel, West Africa, and the Horn of Africa.

⁸⁵ Institute for Economics & Peace, *Global Terrorism Index 2025: Measuring the Impact of Terrorism* (Sydney: Institute for Economics & Peace, March 2025), <https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf>.



Several countries, in particular, have both comparatively high smartphone use, increasing Internet penetration rates and are, unfortunately, significantly affected by terrorism.⁸⁶ These countries constitute, in a way, those potentially most impacted by the future intersection of terrorist use of the Internet and gaming.⁸⁷

Those countries, in particular, would benefit from rapid attention to safeguarding policies implemented across gaming surfaces. However, the many digitizing states across the continent – including those not affected by terrorism – would still benefit from learning how to protect gaming as a safe refuge for play, community, and connection. Gaming also has a transnational dimension and therefore enables cross-border reach, which in turn offers violent extremist actors the ability to connect with communities they might not otherwise have access to. This aspect reinforces the urgency for safeguarding policies not only in terrorism-affected countries, but also in other rapidly digitizing Member States across the region.

A failure to do so will likely result in some, if not all, of the threat scenarios discussed in this paper becoming a reality. Increased radicalization to terrorism, recruitment into violence, and real-world deaths will come as a result.

To mitigate that threat, we recommend that Member States and UN partner implementing agencies draw on the recent three-part framework for mitigating violent extremism on gaming platforms developed by the Extremism and Gaming Research Network (EGRN) and the Global Internet Forum to Counter-Terrorism (GIFCT) as mentioned earlier in this report.⁸⁸ These are grouped into three main categories, which are outlined below in relation to the threat models developed for this Africa-centred research: Prevent, Detect, and React.

⁸⁶ Data from IEP report (above) and GSMA Intelligence, *The Mobile Economy 2025*, GSMA, February 2025, <https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2025/02/030325-The-Mobile-Economy-2025.pdf>.

⁸⁷ Data from IEP report (above) and GSMA Intelligence, *The Mobile Economy 2025*, GSMA, February 2025, <https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2025/02/030325-The-Mobile-Economy-2025.pdf>.

⁸⁸ Galen Lamphere-Englund, *Prevent, Detect, and React: A Framework for Countering Violent Extremism on Gaming Surfaces*, Global Internet Forum to Counter Terrorism (GIFCT), February 2025, <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-PDR-Surfaces-1.1.pdf>.



..... **PREVENT:**

Gap: There is a law-enforcement tools and knowledge deficit, as well as insufficient industry safety coverage for trust and safety efforts across African languages and cultures.

Recommendation 1:

- ✘ **Establish a Gaming Safety Africa Hub.** The hub would be situated within a Member State or UN body and convene annual red-team exercises pairing national cybercrime units with the largest mobile publishers operating on the continent.
 - ▶ It could also fund micro-grants for translating trust-and-safety guidance and community standards into languages such as Hausa, Swahili, Amharic and Somali.

Gap: Offline gaming centres may emerge as grooming nodes for violent extremist recruiters.

Recommendation 2

- ✘ **Introduce a Safe Gaming Certification for gaming cafés:** The certification logo would be displayed in-venues, appealing to parents, and would require minimum age verification, Closed-Circuit-Television (CCTV) on voice-chat booths, helpline posters, and completion of mandatory staff training (see *Detect* section).

Gap: Gender-based harassment and misogyny lower resilience to radicalization to violence and serve as pathways to violent extremist narratives.

Recommendation 3

- ✘ **Launch a game-based Safe Lobby for Girls badge programmes, along with developer training modules:** Studios earn the badge by deploying locally-tuned word-filter packs, ensuring visible female-moderator presence, and embedding bystander prompts in top mobile titles across target countries. Developers could also benefit from gender-responsive safety-by-design training (including inclusive character representation and moderation protocols) provided by UN entities.

Recommendation 4

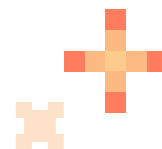
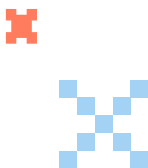
- ✖ **Develop social norm change programmes in gaming to combat violent misogyny**, including positive intervention engagements with live streamers, mentorship programmes with e-sports teams, and community moderator training in how to respond to violent misogyny in gaming.

DETECT:

Gap: Encrypted in-game or café voice chat leaves platforms and law enforcement blind to violent extremist mobilization cues.

Recommendation 5

- ✖ **Roll out a Trusted Community Moderator (TCM) programme:** Through it, government and UN partners can help train café owners, esports administrators and esports leaders and community moderators to recognize concerning gaming-specific behaviours indicative of potential violent extremist conduct and other adjacent harms, such as violent misogyny.
 - ▶ Ideally, this would also provide a lightweight mobile reporting portal or WhatsApp number with a chatbot that triages tips simultaneously to platform trust-and-safety teams and national cyber desks. All participation in programmes should remain voluntary and preserve the privacy and freedom of expression of gamers involved.



Gap: Machine-learning moderation models lack training data and classifiers for violent extremist slang in local languages such as Hausa, Swahili, Amharic, and Somali.

Recommendation 6

- ✘ **Crowd-source violent extremist keyword expansion:** Building on tip lines like those run by Meedan, a CSO dedicated to online safety, this would help to aggregate flagged phrases submitted by the Trusted Community Moderators above into a biannual lexicon update cycle that could be fed into GIFCT or similar industry groups to improve internal moderation efforts.
 - ▶ This effort would share hashes of new terms with member companies to strengthen automated detection in under-resourced African languages.
 - ▶ It could also entail the creation of open-source classifiers based on that lexicon to provide models for small platforms and local start-ups to use for moderation for free-to-low cost.

REACT:

Gap: Gaming platforms and centres lack rapid mechanisms to escalate concerns to psychosocial services or other services that can support victims of online harassment and individuals on the path to or already radicalized to violence.

Recommendation 7

- ✘ **Establish a Referral Network with Psychosocial Services and Providers.** This network would support victims of online harassment and individuals on the path to or already radicalized to violence whenever possible, and provide free resources in contexts where such services are not available.
 - ▶ This system, building on efforts by the Violence Prevention Network (VPN) and Moonshot, could anonymize “user-of-concern” alerts from the TCM programme to reach regional support NGOs within 24 hours.

In areas where there are no support NGOs, this system could provide alternative free de-escalation resources.

