ISD | Powering solutions to extremism, hate and disinformation

ALFRED LANDECKER FOUNDATION

Online Safety and the Regulation of Gaming Platforms and Services

ALFRED LANDECKER
FOUNDATION

ISD Powering solutions to extremism, hate and disinformation

Amman | Berlin | London | Paris | Washington DC

www.isdglobal.org

About the Digital Policy Lab

The Digital Policy Lab (DPL) is an inter-governmental working group focused on charting the policy path forward to prevent and counter the spread of disinformation, hate speech, and extremist and terrorist content online. It is comprised of representatives of relevant ministries and regulatory bodies from liberal democracies. The DPL aims to foster inter-governmental exchange, provide policymakers and regulators with access to sector-leading expertise and research, and build an international community of practice around key challenges in the digital policy space. We thank the Alfred Landecker Foundation for their support for this project.

About this Paper

As part of the DPL, the Institute for Strategic Dialogue (ISD) organised working group meetings between May and July 2024, on the topic of online safety and the regulation of gaming platforms and services. The working group consisted of DPL members representing national ministries and regulators from Australia, Germany, New Zealand, Slovakia, the European Commission, the UK and the US. Participants also included representatives from civil society and academia. While participants contributed to this publication, the views expressed in this paper do not necessarily reflect the views of all participants or any governments involved in this project.

About the Authors

Ellen Jacobs is a Senior Digital Policy Manager for ISD US. She focuses on mitigating the effects of online harms – including those from disinformation, extremism and hate speech – by advancing ISD's digital policy and tech accountability objectives. In her role, she represents ISD to a diverse array of stakeholders including elected officials, NGOs, academics, researchers, and others interested in platform accountability and regulation. Prior to joining ISD, Ellen was at the Omidyar Network, where her funding and advocacy work focused on issues related to platform accountability and open-source technologies. Ellen holds an MIA in Human Rights and Humanitarian Policy from Columbia SIPA and a BA in International Studies from the University of Chicago.

Ella Meyer is a Digital Policy and Platform Accountability Intern for ISD US. In her role, Ella tracks federal and state-level digital policy developments, conducts research on violative content across social media platforms, and incorporates these findings in policy recommendations. She also supports the DPL. Prior to joining ISD, she interned at the University of Maryland's National Consortium for the Study of Terrorism and the Responses to Terrorism, where she supported the Profiles of Individual Radicalization in the United States (PIRUS) dataset. Ella holds a BA in International Relations, and a BA in Russian Language and Literature from The Ohio State University.

Helena Schwertheim is a Senior Digital Policy and Research Manager and leads the Digital Policy Lab (DPL), an intergovernmental working group focused on policy responses to prevent and counter disinformation, hate speech and extremism. As part of the Digital Policy Team, she advises key governments, international organisations and tech companies, and collaborates with ISD's Digital Analysis Unit to translate research into actionable digital policy recommendations. Her particular focus is on Technology Facilitated Gender-Based Violence (TFGBV). Previously, Helena managed digital policy and research projects at Democracy Reporting International. She also has experience working in risk and political analysis in international organizations and think-tanks, including the UN World Food Programme in Rome and the think-tank International IDEA in Stockholm.

Melanie Döring is Project Coordinator for the DPL. She is part of ISD's Digital Policy team, regularly attending meetings to advise policymakers and the German government. Previously, Melanie worked in German Development Cooperation (GIZ)'s Sector Project International Digital Policy, the European Parliament, and an international agency for public relations and public affairs. She holds one MSc in European and International Governance from the Vrije Universiteit Brussels and another in European Integration from the Brussels School of Governance. She also holds a BA in Communication Science and Political Science from the Johannes Gutenberg-Universität Mainz.

Terra Rolfe was a Digital Policy Associate at ISD UK, where she primarily supported the work of the DPL. Terra also supported ISD's global digital policy work, with a focus on Artificial Intelligence (AI) policy. Prior to joining ISD, she interned at the Amsterdam-based civil society organisation ALLAI, advocating for responsible AI legislation in the EU. She holds a BSc (Hons) from Leiden University and is currently an MSc candidate at the Oxford Internet Institute, University of Oxford.

Acknowledgements

We would like to thank all participants of the working group, including experts from governments, civil society, academia and industry, for their contributions. We would like to give special thanks to the speakers and contributors to this paper for their valuable insights and feedback: Dr Jessica White (Acting Director, Terrorism and Conflict, Royal United Services Institute; Co-Founder and Co-Convenor, Extremism and Gaming Research Network), Dr Rachel Kowert, Elsa Isaksson (PhD candidate, Lund University, Swedish Psychological Defence Research Institute), and Charlotte Mariën (Policy Officer, DG Home, European Commission). We would also like to thank ISD colleagues Henry Tuck, Christian Schwieter and Jacob Davey who reviewed this paper.

Contents

Executive Summary

The global gaming industry is now worth more than both the film and music industries combined, with an estimated 3.2 billion gamers worldwide. As such, greater attention has paid in recent years to the online safety risks associated with gaming.[1] This includes both gaming-specific companies and the wider ecosystem of gaming-adjacent social media platforms, particularly in the context of online hate and misogyny, extremism and radicalisation, and child safety issues (such as grooming and cyberbullying).[2] Significant progress has been made in understanding how online harms are perpetrated in online gaming spaces. Recognising these risks, policymakers have crafted new digital and online safety regulations such as the EU's Digital Services Act (DSA) and the UK's Online Safety Act (UK OSA) to increasingly apply to gaming or gaming-adjacent companies. However, such regulations are still in the early stages of implementation and enforcement, and the extent to which gaming companies or services are within scope can be unclear.

This policy brief provides a summary of the current evidence on the nature and extent of these risks and highlights remaining gaps and challenges to building out this evidence base. It also provides an overview of existing government approaches to enhancing online safety in gaming, including both regulatory and non-regulatory efforts, as well as industry and civil society initiatives. Special attention is given to existing regulatory frameworks in the EU (DSA, Terrorist Content Online Regulation), the UK (UK OSA) and Australia (Online Safety Act), to understand how and how far they may provide higher standards of online safety to gamers. Finally, the brief explores both existing and proposed mitigation strategies to enhance online safety in gaming.

Throughout, the brief provides recommendations for governments, regulators, researchers and industry. The DPL supports collaboration through a multi-stakeholder approach to develop a better understanding of the risks posed in online gaming spaces and how best to mitigate them.

Recommendations

Recommendations for Governments

- **Governments should ensure that online safety and tech regulations sufficiently cover all types of gaming companies and gaming-adjacent platforms that pose risks to online safety**: Core online safety requirements – such as the need for platform policies, consistent enforcement and transparency reporting – are obligations applicable to many online services in some jurisdictions including the EU and UK. However, the extent to which online games, gaming companies and (some) gaming-adjacent platforms/services are within scope is often unclear. Where regulation is already in place, online safety regulators should provide clear guidance on which companies, services or platforms are in-scope, and what their resulting obligations are. If it is determined that certain types of gaming companies or services are not covered but could pose significant online safety risks, governments should consider whether legislation should be updated. In contexts where legislation is still being considered or developed (such as the US or Canada), governments should ensure that gaming companies and gaming-adjacent platforms that pose online risks are required to at least meet basic obligations. These include transparency reporting, the moderation of illegal content, the protection of children and some level of data access for external scrutiny (see below).

- **Governments should require gaming-related companies to provide a minimum level of data access for external researchers and regulators**: In contexts where there is no regulation mandating a sufficient level of data access for researchers (such as the US), lawmakers should introduce legislation to close this gap. Where existing legislation falls short, governments should consider whether changes are required to ensure adequate publicly available data access for regulators and researchers in civil society and academia, at least for the largest and most relevant gaming platforms, while ensuring sufficient safeguards for the privacy rights of users. Currently, there is no clear avenue for public researchers to access platform or game company data under the UK or Australian Online Safety Acts, though they both provide powers for regulators to request data. In comparison, Article 40 of the EU's DSA provides a framework to facilitate data access to Very Large Online Platforms (VLOPs). This is a commendable start; however, even if some gaming and gaming-adjacent platforms were designated as VLOPs under the DSA, smaller high-risk platforms and services should also be required to provide data access for researchers.

Additionally, for more sensitive data (such as in-game chats) governments should work with platforms and regulators to explore potential approaches and processes that would allow select researchers access to anonymised chat data in a controlled and safe environment where necessary for specific research projects. This would enable independent researchers to help create a more comprehensive understanding of how platforms (particularly gaming and gaming-adjacent platforms) are used by extremist and terrorist groups. It would also offer insights into trends in hate speech and other types of illegal or harmful content. Such an evidence base is key for informing proportionate policy making, for well-crafted and targeted non-regulatory approaches, and for effective regulatory oversight.

- **Governments should ensure effective multistakeholder cooperation between regulators, researchers and gaming and social media companies to facilitate research exchange**: Cross-sector partnerships are essential for understanding and mitigating the harms posed on gaming and gaming-adjacent platforms. Governments should provide resources for and participate in existing initiatives, such as the European Union Internet Forum (EUIF) and the researcher-led Extremism and Gaming Research Network. These allow regulators, researchers, gaming companies and gaming-adjacent platforms to share research findings and develop strategies to mitigate gaming-related online safety risks. Various industry-led multistakeholder initiatives also exist, including the Global Internet Forum to Counter Terrorism and the Fair Play Alliance. Governments can use these to encourage broader participation from key companies across the gaming industry. Finally, governments should consider providing additional support to existing civil society and academic research networks that focus on gaming-related online safety risks, given the scale and complexity of the gaming sector and the number of gamers around the world.

- **Governments should develop and fund gaming-specific educational and prevention programmes**: To ensure a proactive and holistic approach to mitigating risks and harms related to video games and gaming-adjacent platforms, governments should support educational and prevention programs that are comprehensive and address the diverse needs of the gaming community. These programmes should teach video game users how to recognise risks in online gaming spaces. They should also be tailored to different demographics such as minors and parents, and should help parents and guardians of young gamers to recognise anti-social and extremist rhetoric and behaviour.

Recommendations for Gaming Companies and Gaming-Adjacent Platforms

Gaming companies and gaming-adjacent platforms should adhere to relevant regulations. However, they should also ensure their terms of service are consistently enforced, enact efficient reporting mechanisms for users to flag violative or harmful content, and foster collaboration with policymakers and researchers by facilitating and participating in information-sharing initiatives.

- **Create and consistently enforce clear terms of service and provide effective reporting mechanisms**: Ensure that terms of service are presented to users clearly and predictably, and that they are consistently enforced. Content moderation and trust and safety teams should be adequately resourced. User-reporting mechanisms should be easily located and user-friendly. If companies adhere to their own terms of service, the likelihood will increase that users will trust them to review and act on user reports, making this more effective as well. If they do not do so already, terms of service should also include specific provisions for terrorist and extremist content, hate speech, gender-based violence, child safety, and foreign information manipulation and interference (FIMI), which should be developed in partnership with external issue-area experts.

- **Increase the transparency of moderation efforts and standardise transparency reporting**: Gaming companies should provide at least annual public reports on their content moderation efforts, regardless of whether this is part of the regulation in their specific jurisdiction. This should include measures taken to address content and behaviour which violates their policies. Companies should provide clear public information on the number and language capabilities of content moderators. This transparency should extend to the methods used to moderate content (including automated means). Companies should collaborate with each other and relevant researcher, civil society and government stakeholders on cross-industry initiatives to standardise transparency reporting, ensuring that reports adequately demonstrate compliance with existing laws and provide essential information for public interest researchers focused on tech safety and accountability.

- **Increase public data access for researchers**: Voluntarily enable adequate and standardised data access to researchers on publicly available data. The types of data and metrics available via different Application Programming Interfaces (APIs) should, where possible, be standardised to allow for meaningful cross-platform comparisons.

- **Apply a victim-survivor-centred approach**: Taking a victim-survivor-centred perspective, the development of user interfaces and tools should apply a trauma-informed lens throughout all stages of game or platform development. Companies should adopt proactive measures that support user agency with tools that protect their privacy and reduce exposure to online harms such as hate and discrimination, and accountability measures that deter perpetrators appropriately.

- **Embed Safety by Design throughout product lifecycles**: A Safety by Design approach can help gaming companies and gaming-adjacent platforms mitigate potential user safety issues from the design phase. When developing and releasing new products, services or features, the relevant company should seek to understand, assess and address potential harms instead of retrofitting safeguards after harms occur. A proactive approach toward user safety protects users and mitigates the risk of reputational and financial harm resulting from incidents of online harm (for example, the cost of retroactively introducing technical safety measures).

Recommendations for Independent Researchers

- **Expand the regional focus of research into gaming risks**: Public interest researchers should prioritise expanding the regional focus of studies on the risks posed in online gaming spaces to include a wider range of countries and languages beyond the US, European or other Global North contexts.

- **Collaborate and coordinate with government and industry to develop a common understanding and typology of risks found in online gaming spaces**: Initiatives such as the Fair Play Alliance's "Disruption and harms in gaming framework" are commendable efforts in building an industry-wide shared language and knowledge base. However, this also requires input from and collaboration with independent researchers, regulators and governments.

Glossary

Disinformation

Disinformation is false, misleading or manipulated content presented as fact that is intended to deceive or harm.

Extremism

Extremism is the advocacy of a system of belief that claims the superiority and dominance of one identity-based 'in-group' over all 'out-groups.' It propagates a dehumanising 'othering' mind-set that is antithetical to pluralism and the universal application of human rights.

Foreign Information Manipulation and Interference (FIMI)

FIMI is defined by the European Union Agency for Cybersecurity (ENISA) as "a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory." ENISA explains that the term FIMI aims to refine the concept of disinformation by emphasising "manipulative behaviour, as opposed to the truth of content being delivered."

Hate (Speech)

Hate is understood to relate to beliefs or practices that attack, malign, delegitimise or exclude an entire class of people based on protected or immutable characteristics, including their ethnicity, religion, gender, sexual orientation, or disability. Hate actors are understood to be individuals, groups or communities which actively and overtly engage in the above activity, as well as those who implicitly attack classes of people through, for example, the use of conspiracy theories and disinformation. Hateful activity is understood to be antithetical to pluralism and the universal application of human rights.

Identity Fusion

Identity fusion is a deep sense of personal alignment with an abstract group, cause, or people.[3] It is distinct from other forms of alignment with groups such as group identification in that it particularly emphasises the personal self and relationships to other group members. Measures of identity fusion are strong predictors of extreme pro-group behaviour, such as endorsing fighting or dying for in-group members.

Misinformation

Misinformation is false, misleading or manipulated content presented as fact, irrespective of an intent to deceive.

Online gender-based violence (OGBV)

OGBV is a subset of technology-facilitated gender-based violence (TFGBV). TFGBV refers to any "act that is committed, assisted, aggravated or amplified by the use of information communication technologies or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political, or economic harm, or other infringements of rights and freedoms."[4]

Radicalisation

Radicalisation is a term used in this context to describe the process by which an individual adopts an extremist ideology (defined above), which may (or may not) enable acts of violent extremism or terrorism. In the literature on terrorism and violent extremism specifically, a frequent distinction is made between cognitive radicalisation (adopting extremist beliefs) and behavioural radicalisation (the process leading up to violent behaviour).[5]

Introduction

Over the past few decades, gaming has grown into an industry of impressive magnitude. With 3.2 billion people globally playing games in 2023, and a revenue of $188 billion USD generated in the same year, gaming has undeniably become a popular activity across all age groups.[6] Nonetheless, almost nine out of ten children between the ages of 3 and 17 in the United Kingdom played a video game within the last year, underlining their continued relevance for the market.[7]

Video games can positively impact children by teaching them skills like emotional regulation, social connections, and creativity.[8] This stands in contrast to the feared impacts of gaming on minors, which sparked such widespread concern among the public, and particularly parents, in the 1990s that some labelled it a "moral panic".[9] Although research results remain unclear on, for example, the relationship between violent content in video games and real-life aggression, the outrage led to US Senate hearings with gaming industry leaders and threats of comprehensive regulation.[10] Ultimately, a self-regulatory approach was adopted; this dispute underlines a long history of concerns over gaming that are not always based on a solid research foundation.[11]

The popularity of gaming in conjunction with the rise of online communication platforms has also spurred a dynamic network of gaming-adjacent platforms, where people can discuss their favourite games, watch others play and form communities based on shared interest in games. While spaces to find community are generally positive, gaming spaces can also be exclusive or cause members to adopt harmful in-group mentalities. A significant case that underscores the validity of concerns about harms in gaming communities is Gamergate. This misogynistic movement was initiated in 2014 in reaction to a woman reporter's allegedly unethical coverage of the gaming community and quickly led to targeted misogynist attacks against women involved in gaming, and then expanded to target non-white, non-male gamers. Gamergate is often associated with the rise of the so-called alt-right movement. The ideas behind it remain heavily influential in the culture of the contemporary extreme right.[12]

This example of Gamergate showcases a distinctive feature of online games and gaming-adjacent platforms today. They are highly social environments, differing from and yet increasingly resembling social media platforms in design elements, functionalities and user experiences. The strong social and cultural bonds created within gaming, as well as gaming design and functionalities, can be exploited by foreign interference, hate, terrorist and extremist actors.[13] Moreover, so-called "identity fusion" (see Glossary) describes how certain gamers may have trouble separating their online personas from real life. In some extreme cases, this may lead to increased risks of radicalisation and presents a fertile ground for malign actors that seek to disseminate propaganda and hate, polarise and recruit supporters online.[14] Considering the vulnerability of young users on gaming platforms and larger adjacent online ecosystems, these evolving and, as research suggests, increasing threats should be closely monitored and appropriate responses identified and swiftly implemented.[15]

This policy brief outlines the vulnerabilities that are pronounced in online gaming and adjacent platforms and services. It then describes a range of harms which can be found in these settings. These include hate speech, discrimination, and cyberbullying, extremism and radicalisation, as well as information manipulation and foreign interference. This brief does not aim to focus on potential harms stemming from the content of games themselves (unless games are created by extremists); instead, it considers how games, gaming and gaming-adjacent platforms can be misused to intentionally inflict harms on users. This brief is also not exhaustive regarding other prevalent harms in gaming spaces, particularly around child sexual abuse and exploitation specific issues such as grooming.

The main portion of this brief provides an overview of regulatory frameworks in the field of online safety and how they may apply to gaming platforms and related services amid their early stages of implementation. This includes the European Union's (EU) Digital Services Act (DSA), the United Kingdom's Online Safety Act (UK OSA), Australia's Online Safety Act (AU OSA). It also considers current proposals in the United States such as the Kids Online Safety Act (KOSA) and Canadian proposals. Furthermore, this policy brief explores specific pieces of legislation relating to certain online harms, such as the EU's Terrorist Content Online Regulation

(TCO). It highlights several gaming-specific or gaming-related non-regulatory responses such as the Fair Play Alliance or the EU Internet Forum.

Additionally, this policy brief reviews some of the most common mitigation measures that have been applied to date in gaming contexts. Along with numerous researchers in the field, this brief argues that gaming companies and gaming-adjacent platforms should take stronger action to assess and mitigate risks to curb harms spread on their services.[16] Finally, the brief provides a series of recommendations for the gaming industry, policymakers, regulators and researchers.

Typology of Gaming Platforms and Services

Today's online gaming environment consists of a large range of companies and different types of platforms and services. Table 1 depicts a typology of gaming specific and gaming-adjacent companies, platforms and services with brief descriptions and indicative examples to map out this ecosystem. Some companies may fit under multiple categories, or have different divisions or subsidiaries that provide different types of services.

This first typology demonstrates the diversity in the types of companies, services and platforms involved in the gaming sector. Some span multiple categories, illustrating the complexity of the field and the difficulty in assessing whether or to what extent regulation covers companies (see below, Table 2). In this context, it should also be stressed how different platforms, services and company products are often used in combination. Firstly, they are used to access and play games. This may be supplemented with the use of gaming-adjacent platforms such as forums or livestreams to interact with others.

(Sub)type		Short Description	Key Actors / Examples
Gaming specific	Games and gaming platforms[17]	Enable interaction with "simulated virtual environments"[18] and often with each other, e.g. via in-game chat	Roblox, Minecraft, Apex Legends, PUBG, Fortnite, Counter-Strike, Destiny, Call of Duty, League of Legends, Grand Theft Auto, Helldivers, Diablo, Sea of Thieves, Forza Horizon, Halo, etc.
	Game studios/ developers	Design, test and create games	Riot Games, Epic Games, Activision Blizzard
	Game publishers	Finance, market and distribute games developed by studios	Activision Blizzard, Sony Interactive Entertainment, Tencent Games, Nintendo, Microsoft, Valve Corporation, Take-Two Interactive, Bethesda Softworks, Electronic Arts (EA), Ubisoft, Netflix
	Game markets	Spaces where video games are sold and bought, thus potential gatekeepers (e.g., regarding games produced by extremists)	Steam, GOG.com, itch.io, GameFly, Xbox's Microsoft Store, PlayStation Store, My Nintendo Store, Nintendo eShop, Apple App Store, Google Play Store, Epic Games Store, Green Man Gaming, Kinguin
	Hardware manufacturers	Produce consoles or other physical equipment required for gaming, thus potential gatekeepers	Nvidia, Intel, AMD, Oculus, Asus, Razer, Alienware/Dell, Microsoft (Xbox), Sony (PlayStation), Nintendo, Apple (e.g. iPhone)
Gaming-adjacent	Livestreaming platforms	Enable real-time video-sharing and consumption and often real-time interactions	Twitch, YouTube Live / YouTube Gaming, Facebook Watch/Facebook Gaming, Instagram Live, Kick, TikTok Live, Rumble, Younow, DLive, Trovo, Steam
	Video platforms	Enable the upload and public display of video material, usually with options to comment, like and share	YouTube, Vimeo, Ultreo, Dailymotion, DTube, PeerTube, Odysee, Lbry, Bitchute
	Gaming forums and messaging platforms	Allow for posting messages in open fora, e.g. to ask and answer questions, and/or sending messages	Discord, Reddit (r/gaming), IGN Boards, Minecraft Forum, GameFAQ, Steam, 4Chan, 8Kun

Table 1: Typology of gaming platforms and services with brief description and key actors as examples. Adapted from GNET (2023)[19] and Ofcom (2024).[20]

Threat Landscape: Risks in Online Gaming

Specific features of online gaming spaces create a unique set of vulnerabilities. Several different online risks are frequently present in these environments, albeit to a greater or lesser extent. Risks such as hate speech and discrimination, particularly against women and other marginalised groups, are more common. Risks related to extremism and radicalisation, and foreign information manipulation and interference (FIMI) are typically more sporadic. An overview of the current evidence on each of these risks is outlined below.

Hate Speech and Discrimination

Hate speech and discrimination is of particular concern in peer-to-peer interactions between gamers. This includes sharing hate speech or harassing other players in a targeted manner to intimidate or silence individuals or certain groups. This is often based on discrimination or bias against their race, religion, ethnicity, immigration status, sexual orientation, gender, sex, or disability.[21] Evidence suggests that hate, harassment and so-called "toxicity" is rampant in online gaming platforms and spaces.[22]

A 2023 survey by the Anti-Defamation League (ADL) of online multiplayer gamers in the US found that hate and harassment are so widespread in gaming spaces that they could potentially be perceived as normal.[23] The study cites several variations of harassment, such as publishing private data to expose others to harm (doxing), cyberbullying and trolling. These online interactions can have serious offline impacts: some players reporting negative repercussions on their mental health from witnessing or being a target of hate and harassment, such as feelings of isolation, anxiety, depression and suicidal ideation.[24]

Marginalised groups, such as women and people of colour, are disproportionately affected by hate and harassment.[25] Hate and harassment targeting women on online gaming platforms and services can be understood as a form of **Online Gender-Based Violence (OGBV)**. In five consecutive annual ADL online multiplayer gamer surveys, women gamers were found to be the group receiving the most hate and harassment, with 48 percent of women gamers reporting targeting based on their gender in 2023.[26] Furthermore, OGBV in gaming may encompass extreme cases, such as non-consensual sharing of images, and can extend beyond gaming-related platforms to offline stalking and physical violence.[27]

Due to the damaging effects of such attacks to mental, and potentially physical, health, there is a risk that women gamers are pushed out of gaming environments. 65 percent of women gamers reported they experienced toxicity in gaming while 25 percent reported they avoided certain genres of games due to their negative environments.[28] This is especially concerning as gaming can serve an important role in women's lives, whether as a hobby, develop and host their social circle or even their job (more women playing online multiplayer games today than pre-pandemic).[29] Despite 41 percent of gamers in the US and 40-45 percent of gamers in Asia being women, many players still view gaming as a primarily male domain.[30] The Global Network on Extremism and Technology points to a "propagation of toxic masculinity in gamer cultures".[31] Women being driven from gaming due to toxicity or unsafe environments can potentially have downstream effects and dissuade other women from gaming.

Furthermore, Ukie's 2022 UK industry census showed that just 30 percent of games employees were women.[32] Increasing the number of women employed at games companies can ensure that more diverse and inclusive perspectives are being incorporated into the design and administration of games. This includes instituting policies to make gaming spaces safer for women, or ensuring that more women characters are included in games and are not over-sexualised.[33]

Other marginalised groups are also disproportionately affected by hate and harassment in gaming spaces. The 2023 ADL survey of online multiplayer gamers, which collected data from 4 to 17 August 2023, found that half of Black American adult gamers reported experiencing harassment due to bias or discrimination against their race. 70 percent of Jewish-American adults also reported some form of harassment.[34]

As mentioned in the introduction, another striking example is the Gamergate case: in 2014, this hashtag was initiated to coordinate a targeted harassment campaign against a woman games developer amid her research on diversity in gaming, over alleged ethical grievances. The campaign expanded to target outspoken women in the field. The hashtag became a rallying point for misogynist and radical far-right actors against all those who do not resemble the "classic" image of the white male gamer.[35] In 2021, Vox criticised how the media and society at large dealt with this campaign: although Gamergate was not the start of online extremism, an appropriate response could have set a standard for building resilience or mitigating similar attacks.[36] Instead, the article argued that perpetrators learned they could orchestrate harassment at scale with little fear of repercussions. Media initially downplayed the campaign as "trolling", expecting it to lose traction even as it was forming a key part of the nascent alt-right movement.

Extremism and Radicalisation

In recent years, the connection between video games and extremism has become an increasing topic of concern, especially given reports of extremist groups using video games to connect with like-minded individuals. Extremist groups' games can be an effective way to radicalise those who are already sympathetic to the groups' views, but they are generally ineffective at reaching those who are not.[37] For example, Hezbollah released the video game "Sacred Defence – Protecting the Homeland and Holy Sites" in 2018.[38] The game, which was available for purchase in gaming shops in Lebanon, allows players to assume the role of a Hezbollah fighter in major battles against the Islamic State (IS).

Another way for extremist groups to connect with potential sympathisers is through their own modifications, or "mods", to existing games and in-game chat functions. Examples include a map populated with extremist group symbols and narratives.[39] Mods provide such a "powerful immersive quality" to video games that they have "been effective at inspiring and allegedly training extremists to perpetrate real-world attacks".[40] Extremist groups also exploit the in-game chat feature to find ideologically sympathetic individuals. Extremist group recruiters may use discriminatory jokes "to identify like-minded individuals without giving away their cause.... By leveraging jokes, extremist actors can help to facilitate a 'cognitive opening', which can be used to create a conversion funnel to more private settings".[41] Notably, extremist groups use in-game chats as a recruiting tool, because they are less moderated and less regulated than other online platforms, like social media.[42]

Outside of video games, gaming-adjacent platforms like Steam (which is also a game market), Twitch or Discord, can serve as a conduit for extremist groups to connect and maintain strategic relationships. These types of platforms have often been the recipients of cross-platform migrations from larger platforms as prominent extremist users or communities have been deplatformed elsewhere. Whether these communities have direct connections to online gaming or not, these platforms can be attractive due to the social media and private communication functionalities they offer, alongside less effective or consistent moderation.

Extremist channels on gaming-adjacent platforms can easily be found with a simple search, suggesting a lack of effective and consistent enforcement across the online gaming ecosystem. In a study conducted by New York University, researchers found that extremist channels openly advertise their ideology. In one case, researchers found a Discord channel that openly used neo-Nazi symbols and codes in its public tags, including 88 (numerical code for the Nazi salute, "Heil Hitler").[43] The server also promised its channel members access to a network of neo-Nazis that has "many members and is active all the time".[44] Previous ISD research found minimal evidence of extremist recruitment on gaming-adjacent platforms, though they may still be used to host active and long-lasting networks of extremists, including violent ones.[45]

Other gaming-adjacent platforms including DLive and Kick are popular venues for extremist individuals and groups to connect after being removed from more mainstream gaming-adjacent platforms like Discord, Steam, and Twitch. DLive, for instance, hosted many well-known leaders from the white nationalist movement who regularly used the platform to raise money. Nick Fuentes, a prominent white nationalist, earned over $68,900 USD in a six-month period in 2020 on the platform.[46] DLive awards users 'lemons' for watching livestreams, which then can be donated to extremists like Fuentes (each lemon equalled $0.012 USD at the time that Fuentes was an active live streamer).[47] However, DLive faced intense scrutiny after multiple individuals livestreamed themselves storming the U.S. Capitol on January 6th, 2021.[48] In response, DLive began to more strictly regulate content, leading to an exodus of extremist streamers from the platform.[49]

In 2022, Kick, a new video game streaming platform, was launched. Kick is known for its minimal content moderation, making it an attractive platform for extremist streamers.[50] An analysis of the platform by the Global Network on Extremism and Technology (GNET) found that right-wing extremists and conspiracy theorists were able to freely create and distribute content. GNET researchers believe that both Kick and DLive serve a role in the dispersal of far-right extremist narratives and conspiracy theories on an international scale.[51]

Foreign Information Manipulation and Interference (FIMI)

Online games and gaming-adjacent platforms can also be exploited for foreign information manipulation and influence (FIMI), though this area remains largely under-researched as of now. In a pioneering 2023 report, the Swedish Psychological Defence Research Institute assesses FIMI threats and vulnerabilities on gaming platforms focusing on tactics, techniques and procedures (TTPs) specifically within gaming.[52]

The researchers understood information influence as "a form of cognitive influence conducted by foreign powers [...] to influence the perceptions, behaviour, and decisions of target groups to [their] benefit", and acknowledges that this tends to appear in the form of coordinated campaigns. While the report found that sufficient data on FIMI in gaming was limited and that it was difficult to attribute attacks, it provides a useful taxonomy in grouping more than 40 identified FIMI techniques into six overarching tactics:

1. Reframing reality to dispute historical facts or utilising video gaming imagery to represent actual situations.

   For example, in 2017, open-source research network Bellingcat debunked claims made by the Russian Ministry of Defence across several social media platforms which used video game imagery as "proof" that the was US collaborating with Islamic State (IS).[53]

2. Projecting authority to use games as tools for influence.

   For example, authoritarian actors may buy studios or pressure the industry to align with their values for market access, within the wider context of ideological competition.[54]

3. Hacking or phishing attempts by malign actors to retrieve data that can then be used against the entire gaming ecosystem.

4. Interactive propaganda aiming to disseminate ideology via the development of the actor's own games, or in-game narratives or advertisements in existing games to influence beliefs and gain new supporters.

5. Social propaganda attempts to create in- and out-group dynamics across gaming platforms, often in preparation for ideological shifts.

6. Psychographic targeting may include using data points or entire datasets to improve profiling and tailor content to the most influenceable audiences.[55]

In September 2024, the US Department of Justice (DOJ) seized 32 internet domains linked to the Doppelganger disinformation campaign. The documents released as part of the DOJ's announcement showed a plan to manipulate the outcome of the US 2024 presidential election, which included potentially targeting American gamers, Reddit users and those who used image boards.[56] This audience was described in documents as the "backbone of the right-wing trends in the US segment of the internet".[57]

Challenges to Understanding the Threat Landscape

Grasping the full extent and impact of online harms from foreign interference, hate, and terrorist or extremist actors on gaming platforms and services remains a significant challenge. The lack of data access and comparability significantly impedes the types of research needed to fully map the threat landscape.

This is due to a variety of factors, including the sheer volume and diversity of types of user-to-user interaction. This can obscure malicious activities, especially in real-time communications, creating a challenge for the collection and analysis of data. Furthermore, the platforms on which these interactions take place impacts the level of access for researchers. For example, chats can vary between being public (relatively easy to access but potentially difficult to collect at scale), private (where access may need to be applied for or managed, if available at all), or encrypted (largely inaccessible unless directly infiltrated).

Interactions may also occur beyond gaming platforms themselves on gaming-adjacent platforms like Discord or Twitch. While these types of platforms may offer greater data access opportunities, they are still relatively limited. This is especially true for more private spaces or ephemeral content such as livestreams. This makes tracking users or their interactions across platforms particularly challenging for researchers.[58] This cross-platform nature of online gaming communities may be exploited, as extremists often seek to use gaming communities to build networks of sympathetic users before encouraging them to move to sites which are less heavily monitored.[59]

Cross-platform use highlights the need for more data, but also for better transparency reporting from the gaming industry. These reports are increasingly required of online service providers in new regulation (such as the EU's DSA); they may provide insights on industry actions such as content moderation, user reporting, and account banning. However, many gaming companies have only begun issuing transparency reporting recently. A lack of consistency across the industry making comparisons between them difficult.[60] One report noted in 2023 that "9 of 14 leading gaming companies in the USA have made no public efforts to assess or mitigate extremist content in their products".[61]

Another challenge is the lack of a common language among researchers for understanding the levels of "toxicity" or harm in video games, making it difficult to determine and compare the prevalence of harmful actions across spaces and time.[62] Existing taxonomies differ on the scale and types of harm, and the cut-off points and differentiations of types of harms. A shared language and knowledge base among researchers, industry and policymakers is integral for understanding the threat landscape but also for any successful interventions.

Furthermore, there limited research on gaming experiences from intersectional perspectives, such as gender and ethnicity. Based on the literature review and conversations conducted with experts for this brief, this is an underserved area of research. Incorporating intersectionality in further research, including the unique harms that gamers with these characteristics face, will provide a more robust understanding of the field overall.

Finally, some reports note that hateful or toxic behaviour is so commonplace in many users' gaming experiences, and that it is being normalised and increasingly viewed as an "accepted part of gamer cultures".[63] This is worrying for several reasons, not least that normalisation may lead users to not see this behaviour as harmful, impeding user reporting or surveys. This might make understanding the scale and scope of harms in online gaming environments much more difficult, particularly regarding the experiences and harassment of women and minority gamers.

Features and Vulnerabilities of Online Gaming Platforms

Design Vulnerabilities

In the context of the harms covered by this brief, several gaming design features are particularly vulnerable to exploitation by foreign influence, hate, extremism or terrorist actors. Five features of game designs are particularly vulnerable:

- The game design, which will influence size of gaming communities, their demographic including use by young users and the opportunities for interaction,
- The role of user-generated game elements,
- Inadequate moderation and reporting functionalities,
- Parental controls,
- Built-in monetisation opportunities.

While the gaming industry has not yet faced a major scandal regarding information influence or manipulation, researchers warn it is "ripe with vulnerabilities" for information exploitation, and remains an attractive venue for hate, terrorist and extremist activities.[64]

Cross-platform gameplay capabilities and community interaction tools bring many people into contact with one another. Cross-platform gameplay enables users to connect through different consoles or platforms.[65] While not all games are massively multiplayer online games (MMOs), almost all offer community interaction tools such as on-platform text, voice or audio chats.

Many chats are encrypted, limiting platforms' options for moderation. Chat security and encryption can vary based on the game or platform; it also appears that some companies can access and decrypt user communications.[66] However, companies' relative lack of oversight means that such functions are a straightforward way to initiate communication with sympathisers and potential recruits to hate, extremist and terrorist groups.[67] Gaming-adjacent livestream and messaging platforms also provide pathways for users to communicate – and radicalise – each other; for example by sharing increasingly radical content and livestreaming acts of violence.[68]

User-generated or modified elements of games, such as "skins," user-built worlds, and modifications or "mods" are also vulnerable to exploitation. Skins change the appearance of models within a game and have been used within first-person shooters – for example to add references to the Nazi party or Islamist terrorist groups.[69] Features that allow users to create independent worlds similarly allow users to enact extreme and hateful fantasies virtually.[70] For example, players have simulated Nazi concentration camps and Uyghur detainment camps in Roblox and Minecraft, as well as re-enactments of the Third Reich and IS in roleplaying simulations.[71]

Mods go further by adapting the narrative, iconography and aesthetics of existing games. As such, they can be exploited to fit the ideology of terrorist, extremist, hate or foreign influence actors.[72] They are available via third-party websites, such as gaming forums and pirating websites and are considered more popular and user-friendly than developing wholly new games.[73] Mods often have low-production value, with the possible exception of games created by hostile state-backed development studios.[74] It should be noted that despite their vulnerability to exploitation, manipulated skins and mods do remain a small fraction of material. Mods have been used to create propaganda, such as mods to a first-person shooter game that made Islamic State fighters heroes instead of villains.[75] Violent extremist or terrorist groups can also use mods to violent games to desensitise members to extreme violence, or to train and prepare for combat or attacks.[76]

The exploitation of gaming platforms detailed above is exacerbated by a lack of consistent and effective **content moderation and reporting mechanisms**, which parallel issues faced by social media platforms. Most platforms have terms of service prohibiting certain content and behaviours; however enforcement is challenging due to the high volume of content, and gaming design elements. Gaming companies often do not adequately fund and staff moderation efforts, and some appear to make little effort to moderate their platforms.[77] Researchers have also argued that the engagement generated by hateful activity may be profitable for companies, whereas moderation is costly.[78]

Content moderation often combines automated detection with human oversight. Many games offer both text and voice communications between users, which often require different approaches to content moderation. Despite continued reports of harassment in voice chats, platforms have been slow to enact changes to address these. Some companies, such as Riot Games and Activision Blizzard, have begun to record or moderate in-game voice communications in specific games.[79]

Automatic moderating (such as text or key-word filtering), identifying threats automatically and moderating harmful speech can be difficult as references in some games where guns or violence are common.[80] For example, "I will kill you" can be an entirely acceptable thing to say within a game but could also be an actual threat of offline violence.[81] These moderation difficulties can be purposefully exploited by threat actors. In some instances, they may continue communicating via such channels even once banned on other mainstream platforms.[82] Furthermore, even when there are options for players to report harmful or violative actions from other players, many are deterred because they believe it is an ineffective method for removing those players or subsequent follow-up from game administrators.[83]

Parental controls are also often relied on by parents as a solution to safeguard children from hate and extremist content, as well as graphic sexual content and inappropriate interactions with adults. However, these are relatively easy to bypass, even on platforms targeted at younger users such as Roblox.[84] Even if parents are implementing parental control tools, they are often unaware of the full scope of tools available. 81 percent of parents surveyed by Internet Matters said they were implementing a parental control tool; however, of the 7 tools they were asked about, parents were implementing an average of 1.7.[85] Furthermore, even if parents are implementing parental controls, they might only learn about details such as how long their child is playing games on an average day rather than how often they are gaming with strangers. Just three out of ten parents surveyed by Singapore's Ministry of Communications were fully aware of who their child was interacting with when gaming.[86]

Lastly, **monetisation functionalities** within games are an additional design vulnerability and are have become a key part of the gaming industry's business model. In-game currencies and mystery-prize-style "loot boxes" can both have real-world value, including some which can be directly converted into fiat currencies, and therefore risk being exploited by threat actors.[87] A European Commission analysis of terrorism and gaming in 2020 determined that as yet this remains a theoretical vulnerability.[88]

However, lack of regulation and scrutiny leaves monetisation features vulnerable to future exploitation. Loot boxes may be used for money laundering by terrorist or criminal organisations. In-game currencies can also facilitate the transfer of money quickly, easily and with less scrutiny across borders. This may be a particularly attractive feature for threat actors operating in multiple jurisdictions.

Additionally, loot boxes are often aimed at or easily accessible by children. In a UK House of Commons Digital, Cultural, Media and Sport Committee hearing on immersive and addictive technologies in 2019, written evidence from two psychologist expressed "concerns about the 'structural and psychological similarities' between loot boxes and gambling". This included the design element of providing random loot boxes to players as "akin to conventional gambling products [which are] designed to exploit potent psychological mechanisms associated with the development and maintenance of gambling-like behaviours".[89]

While there is not enough evidence to fully conclude a causal link between loot boxes and gambling, this could be an emerging child safety issue.[90] This loot box functionality has also been noted as a potential avenue for grooming children to partake and "normalise" gambling behaviour.[91]

Social and Psychological Vulnerabilities

The strong social and cultural bonds created within gaming communities can be powerful sources of connection and belonging and are often positive. However, foreign interference, hate, terrorist and extremist actors can also exploit these bonds.

Many gaming platforms also offer high levels of anonymity, and some require players to create teams, sometimes with strangers.[92] The strong in-group/out-group dynamics within gaming communities – both between teams and in relation to the outside world – alongside social bonds, can increase the risk of users being radicalised.[93] Anonymous social elements may also allow terrorist, extremist and foreign interference actors to establish contact with users and shape conversations or encourage users to move to less-monitored spaces, where increasingly extreme propaganda or content can be shared.[94] This process can also happen on gaming-related livestreaming or communication platforms such as Discord and Twitch.[95]

The MMO game World of Warcraft encourages players to form virtual "guilds" – communities of players who can come together for a common purpose and in-game activities – some of which have become major hubs for neo-Nazi forum Stormfront. Developer Blizzard indefinitely shut down one of these guilds following sustained criticism from a member of the US Congress in 2019.[96]

Specific psychological mechanisms also increase the risk of radicalisation in gaming contexts. Namely, gamification helps players create and maintain connections with other players while also fulfilling their psychological needs.[97] This is often positive but can also facilitate radicalisation processes when extremist actors exploit gamification. Namely, extremist actors can exploit gamification to increase engagement with extremist content and draw individuals into extremist groups and channels.[98]

Furthermore, due to specific shared stressful experiences and subsequent bonding that often happen in gaming environments, users can also experience identity fusion, another potential avenue for radicalisation.[99] This is predictive of known markers of extremism, such as sexism, racism and endorsement of extreme behaviours including the willingness to die for a cause. This suggests that gaming may play a direct role in radicalising certain users. Studies also show that specific personality attributes (e.g. loneliness) may amplify support for extreme behaviour in the context of gaming.[100]

Existing Regulatory and Non-Regulatory Government Responses

Games have long been criticised over their content and potential addictiveness, especially by stakeholder groups such as parents.[101] The history of regulatory action on games may have created a barrier for effective engagements between industry and government.

The 1990s were marked by public outrage over violent games including Mortal Kombat, Night Trap, and Doom. Media and public outcry prompted US Senate hearings in 1993 and 1994, with industry giants Nintendo and Sega testifying. In response to policymakers' threats of regulation, the gaming industry established the Entertainment Software Association and the Entertainment Software Ratings Board (ESRB) to introduce age ratings. Some companies also adjusted and partially published content policies.[102] The public outcry and debate in the 1990s damaged trust between industry, policymakers and society – a stakeholder relationship that may be difficult to navigate when collaborating on new regulatory approaches.[103]

Age ratings are relatively easy to assign and enforce before a console game is published and sold over the counter. It is much harder to do so in today's increasingly complex and online gaming ecosystem, with user-generated content (including co-creation of virtual worlds), live interaction and online purchases. Thus, the self-regulatory mechanisms adopted in the mid-1990s are now outdated due to both the progression of technology and evolving harms in online gaming spaces.

However, a new era of digital and online safety regulation has introduced legislative frameworks that may increasingly apply to gaming or gaming-adjacent platforms and services. These regulations are still in the early stages of implementation and enforcement, and the extent to which different gaming companies or services are within scope is unclear. The section below outlines key online safety regulations and how they may address online gaming platforms and companies. Further details on each regulation can be found in the Annex.

1 Digital Services Act (European Union, 2022)

The European Union's (EU) Digital Services Act (DSA) is a horizontal legal framework that applies across online harms, harmonising the governance of a wide range of digital services throughout the EU to increase online safety. It takes a staggered approach of due diligence obligations: some apply to all intermediaries while additional duties are imposed based on types and size of services (see Annex). Given the vast landscape of online gaming and gaming-adjacent platforms (see Table 1), it is not immediately clear how DSA obligations apply in some cases (see Table 3 in the Annex). The European Commission noted in a 2023 study on gaming that the DSA "will most likely influence the video game industry in many ways, depending on how video games are categorised under the new rules".[104] The study goes on to say that the latter "may also fall under the scope of the DSA due to the online community features they include. This applies [...] to games featuring important in-game interactions (e.g., custom profiles, in-game chats, possibility to add other users as contacts)". This underlines a degree of uncertainty even from the European Commission itself.

Generally, online gaming companies and gaming-adjacent platforms likely qualify at least as **intermediary services** since simply enabling access to a communication network constitutes a "mere conduit" service. Duties then include ensuring accountability through company points of contact and EU legal representatives and responding to authority orders for illegal content. Additionally, intermediaries must enable transparency through public terms and conditions that outline restrictions on the use of their services. Content moderation practices must respect fundamental rights and be detailed in standardised annual transparency reports.

If information is stored permanently, the service qualifies as a **hosting service**. Obligations include the maintaining notice-and-action mechanisms and providing statements of reasons for restrictions as well as possibilities for users to appeal decisions. Hosting services must also cooperate with Member State authorities when there is suspicion of serious criminal offences.

Depending on the functionalities of a game or gaming-adjacent platform, the company may also qualify as an **online platform** if information is publicly disseminated, e.g. via public in-game chats. This would involve implementing suspension processes for repeated misuse of the service, imposing restrictions on deceptive design and targeted advertising, and enforcing stricter measures to protect minors. Additionally, online marketplaces must further ensure the traceability of traders.

Additional obligations depend on size, as **very large online platforms and search engines (VLOPSEs)** with over 45 million monthly active EU are considered to have a greater potential for online harms. These obligations include crucial data access provisions for vetted researchers, mandatory annual independent audits, and a risk assessment and mitigation procedure. At the time of writing, no major gaming(-adjacent) company has been classified as a VLOP by the European Commission. Significant gaming companies such as Discord, Twitch and Steam claim to have fewer than 45 million monthly active users in the EU.[105] However, YouTube, which hosts a wide range of content including gaming, has been designated as a VLOP.

Overall, case-by-case legal assessments basis are necessary to determine which parts of the DSA apply to each game or gaming-adjacent company.[106] However, the DSA appears particularly relevant for online gaming companies and multiplayer games where significant user interaction is expected.[107] The respective obligations go beyond most of the safety measures and transparency levels currently to be found in the industry.[108]

While not all of the DSA will apply to the entire gaming industry, it may be advisable to still adapt to evolving industry standards by implementing at least basic minimum of reporting options, moderation of content and some level of transparency. Falling short of these expectations could lead to reputational damages and a loss of user trust as expectations rise.[109]

2 Online Safety Act (UK, 2023)

In the UK, the most relevant legislation for regulating online gaming companies is the 2023 Online Safety Act (OSA), which aims to enhance online safety.[110] The UK's communications regulator, Ofcom, defines gaming services as those that "allow users to interact within partially or fully simulated virtual environments".[111] In consultation materials, Ofcom acknowledges that gaming services have been used by terrorists as recruitment and training tools, particularly to recruit minors. It also highlights the use of gaming-adjacent platforms for the promotion and dissemination of terrorism content.[112] The consultation further notes the risks of grooming of minors on gaming services, as well as other forms of abuse including physical threats, stalking and sustained harassment, and hate-related offences.

Gaming platforms and services that enable user-to-user interactions are classified as regulated "U2U" services, and the OSA, which mandates compliance with various duties and responsibilities to protect users from harmful and illegal content.

Specifically, U2U services must adhere to duties of care concerning illegal content and content that is harmful to children. Category 1 services (those with the highest risk features and widest risk) would also have to apply duties of care to other harmful content. They are required to assess the risks associated with their services and implement measures to mitigate these risks. The Act also mandates that regulated services, including U2U gaming companies, establish robust content moderation policies and practices, ensuring moderators can efficiently identify and remove illegal content. Companies with the widest reach must consistently enforce their terms of service around harmful content.

The OSA also includes specific provisions aimed at protecting children from harmful content, which are especially relevant for online gaming. Regulated services likely to be accessed by children must conduct specific assessments to identify potential risks posed by content that is harmful to children; they must also implement appropriate safeguards.

Services must also provide clear processes for users to report harmful content and maintain transparency reports detailing their compliance with the OSA's requirements. Additionally, regulated services are required to follow Ofcom's codes of practice, or implement steps that are as effective, and may be subject to audits and investigations to ensure compliance.

In summary, the requirements on gaming companies under the OSA are relatively explicit and extensive and will require gaming platforms to adjust processes and policies to ensure compliance. As the digital landscape continues to evolve, the implementation of the OSA will serve as a critical benchmark for the ongoing development of regulatory frameworks worldwide. This will emphasise the need for proactive measures to safeguard users, particularly vulnerable populations, in online gaming environments.

3 Online Safety Act (Australia, 2021)

Australia's Online Safety Act of 2021 (the Act) provides protections for Australians online through the removal of harmful online content. It also sets expectations and requirements for industry to make them more accountable for user safety.

The Act provides for mandatory codes and standards covering eight sections of the online industry including social media services, app distribution services, hosting services, internet carriage services, equipment providers, search engine services, relevant electronic services and designated internet services. These codes and standards lay down a set of legally enforceable compliance measures to address systemic issues and reduce the risk of illegal and restricted material circulating. Industry standards for relevant electronic services and designated internet services, drafted by the eSafety Commissioner, are due to come into effect on 22 December 2024. Relevant electronic services include online gaming platforms that enable end-users to play with other end-users. Gaming adjacent platforms may be considered relevant electronic services or be covered by another category depending on the platforms' features.[113]

The Basic Online Safety Expectations aim to improve the safety of Australians online through industry transparency and accountability. Under the Act, the eSafety Commissioner can require social media services, relevant electronic services (including online gaming) and designated internet services to report on how they are meeting any or all of the expectations. These expectations include, but are not limited to:

- Ensuring all end-users can use services safely,
- Having terms of use, policies and procedures for safe use,
- Minimising provision of unlawful and harmful material and activity.

A second set of industry codes focussing are under development by industry associations in Australia. These are designed to prevent children from accessing or being exposed to age-inappropriate material online. Also, they aim to provide users with effective information, tools, and limit access and exposure to such material.

The Act also enables several complaints schemes where Australians can report harmful and unlawful material online to the eSafety Commissioner, and for the eSafety Commissioner to require the removal of seriously harmful material. These include the Adult Cyber Abuse Scheme, Cyberbullying Scheme, Image-Based Abuse Scheme, and Illegal and Restricted Content Scheme.

The mechanisms provided by the Act aim to place the responsibility on gaming companies and gaming-adjacent platforms to anticipate and adapt to emerging threats to online safety for Australians, while still providing a safety net for Australian children and adults through the complaint schemes.

4 Proposed Legislation in the US and Canada

The US and Canada do not have larger regulatory schemes that span multiple online harms comparable to the EU's DSA or the UK or Australian OSAs. However, there has been significant debate in both countries about how to mitigate online harms from social media platforms (particularly those affecting children) through regulation, resulting in some legislative proposals.

There has also been increased awareness of how gaming companies and gaming-adjacent platforms have perpetuated or exacerbated some of these harms, and discussion about ways in which to incorporate those companies into existing legislative proposals. For instance, in 2023, in response to increasing reports of white supremacy and other extremism in online games, Democrat Representative Lori Trahan and other Congressional Democrats requested information from gaming companies on their harassment and extremism policies.[114]

Perhaps the most notable proposal in the US that encompasses gaming and gaming-adjacent spaces is the Kids Online Safety Act (KOSA), a bill that has been introduced in both chambers of Congress.[115] The Senate version, introduced by Senators Blumenthal and Blackburn, has undergone extensive changes since its initial introduction in 2022. The bill proposes a duty of care standard, safeguarding requirements, and mandated disclosure and transparency reports from covered platforms. This explicitly include online video games, social media services, social networks, messaging applications, video streaming services or any other social platforms that connect to the internet and are used by minors.

The Senate version would require these covered platforms to take "reasonable measures" in the operation of their platforms to "prevent and mitigate":

- Mental health disorders (including depression and anxiety),
- Practices that encourage addiction,
- Physical violence, online bullying and harassment of minors,
- Sexual exploitation and abuse, the promotion or marketing of narcotics, tobacco products, gambling or alcohol,
- Financial harms.

It would also mandate certain safeguards, such as limiting who can communicate with children and limitations on features that increase children's time on the platform.

However, the version of KOSA introduced in the House in 2024 contains several important distinctions that would change its effect on online games. The most recent version of the bill, introduced ahead of a cancelled markup[116] in June 2024, adopts a tiered approach: the duty of care of would only apply to "high impact online companies", which have at least $2.5 billion USD in annual revenue or more than 150 million global monthly active users.[117] It also changes the "knowledge" standards – those same platforms would have the strictest requirements around knowing which users are children or minors, and enacting accompanying safety standards. These changes would exclude from smaller gaming and gaming-adjacent platforms from having to design and run their platforms with the same safeguards in place for children.

Several states have introduced or passed bills modelled off the UK's Age Appropriate Design Code, which mandate that companies design their platforms in a way that prioritises child safety and privacy, minimises the amount of data that can be collected and used about minors, and provide transparency to children and their parents about terms of service and parental controls.[118] California became the first state to pass an Age-Appropriate Design Code in the US in 2022, which required "all online products and services [children] are likely to access" to "consider the best interests of children when designing, developing, and providing" that service, which would include gaming and gaming-adjacent companies.[119]

NetChoice, a tech trade association, then sued the State of California on the grounds that the law was unconstitutional.[120] A federal court ruled in August 2024 that requiring companies to anticipate and mitigate risks to children was likely unconstitutional.[121] Despite this, New Mexico, Minnesota, Vermont and Maryland attempted to pass versions of the Age-Appropriate Design Code; Maryland was the only state to pass successfully a law in 2024.

The proposed Online Harms Act (Bill C-63), introduced in Canada in 2024, would establish a regulatory framework. This would include the creation of a Digital Safety Commission to oversee enforcement of the Act and a Digital Safety Ombudsperson who would provide support to users. It would also require social media services to adhere to several duties of care, including risk mitigation, design for the safety of children, and keeping CSAM inaccessible on their platforms.

Social media services are defined as "a website or application that is accessible in Canada, the primary purpose of which is to facilitate interprovincial or international online communication among users of the website or application by enabling them to access and share content". This would likely cover most gaming and gaming-adjacent companies.[122] Under this law, social media services would have to mitigate users' exposure to harmful content, which includes "content that sexually victimises a child or revictimizes a survivor; content that foments hatred; content that incites violence; content that incites violent extremism or terrorism".[123]

The EU's Terrorist Content Online (TCO) Regulation (2021): Regulation Addressing a Specific Online Harm Pertinent to Online Gaming

Unlike the EU's DSA, the Terrorist Content Online Regulation (TCO) aims to curb a specific online harm: the dissemination of terrorist content online. For this purpose, it refers to the definition of terrorist content in the Counter-Terrorism Directive, while extremist content below the threshold of terrorist content is not in scope. The TCO applies to Hosting Service Providers (HSPs), which are defined as storing content at user request and disseminating it to the public. Like the category of platforms under the DSA, the TCO requires a public dissemination of content. Recital 14 provides guidance on what may be understood as "dissemination to the public", entailing that information be made available to a potentially unlimited number of persons, without further action by the content provider, irrespective of whether individuals actually access the information or not.[124] It is unclear which gaming companies or parts of the gaming ecosystem fall under the scope of the TCO, similar to other legislative pieces outlines above; it depends on the functions and features of a service.

Similarly to DSA obligations for intermediaries, TCO requires HSPs to establish a point of contact and legal representative within the EU, and publish terms and conditions as well as annual transparency reports on them. Terms and conditions must state the approach towards curbing the spread of terrorist content. Importantly, HSPs must remove terrorist content within one hour of receiving a removal order by any Member State authorities. These removal orders are binding though may be scrutinised by host competent authorities (or at HSP or user request).

Authorities must be informed about actions taken, and content that has been removed or to which access has been disabled must be preserved for six months. Users must also be informed about removals, and remedies and complaint mechanisms must be available to them, which yet again resembles the DSA. Moreover, HSPs must inform competent criminal prosecution authorities when becoming aware of terrorist content constituting an "imminent threat to life".

In addition, HSPs "exposed to terrorist content" (Article 5) – a status determined by Member State authorities – must implement "specific measures" and report on them. These may include adapting personnel, technical capabilities, or user moderation and reporting mechanisms. When applying these measures, fundamental rights must be considered. Lastly, these HSPs must inform how terrorist misuse of their service is addressed in their terms and conditions.

Some major gaming players such as Twitch and Roblox publish transparency reports under the TCO.[125]

Applicability of Regulation to the Gaming Industry

Finally, Table 2 aims to assess how the previously outlined legal frameworks are likely to affect the gaming industry, usually depending on concrete functionalities.

Table 2: Overview of likely applications of key regulations across jurisdictions to different types of online gaming services.

		European Union: Digital Services Act (DSA)	United Kingdom: Online Safety Act (OSA)	Australia: Online Safety Act (OSA)	European Union: Terrorist Content Online Regulation (TCO)
Gaming specific	Games and gaming platforms	Likely qualifying at least as intermediary services, potentially as platforms depending on functions and features. Obligations depending on size.	In scope (user-to-user services).	In scope where the game enables end-users to communicate to each other online, and share content on the platform.	May qualify as HSP, if dissemination of content to public. For example, Roblox publishes transparency reports under the TCA.
	Game studios/ developers	Yes, if they develop games that qualify at least as intermediaries.	In scope, if game allows online interaction, communication or content sharing.	In scope where the studio/developer is the responsible entity for the in-scope gaming platforms.	Yes, if they develop games that qualify as hosting service providers.
	Game publishers	Yes, if they publish games that qualify at least as intermediaries.	In scope, if game allows online interaction, communication or content sharing.	In scope where the publisher is the responsible entity for the in-scope gaming platforms.	Yes, if they publish games that qualify as hosting service providers.
	Game markets	Likely qualifying as online marketplaces. Obligations depending on size.	In scope, if game allows online interaction, communication or content sharing.	In scope, if the market is an app distribution service, or if it allows online interaction, communication or content sharing.	May qualify as hosting service provider (HSP).
	Hardware producers	Potentially, if they produce products that qualify at least as intermediaries.[126]	In scope.	In scope.	Potentially, if they produce products that qualify as hosting service.[127]
Gaming-adjacent	Live-streaming platforms	Very likely qualifying as online platforms (or DSA already applying, e.g., Twitch[128] publishes some data on DSA transparency obligations). Obligations depending on size.	In scope.	In scope.	Very likely qualifying as HSP (or already applying, e.g., Twitch is[129] publishing transparency reports under the TCA).
	Video platforms	Very likely qualifying as online platforms (or DSA already applying, e.g., VLOP YouTube). Obligations depending on size.	In scope, if platform allows online interaction, communication or content sharing.	In scope.	Very likely qualifying as HSP.
	Gaming forums and messaging platforms	Likely qualifying as online platforms, if public-facing. Obligations depending on size.	In scope (user-to-user services).	In scope.	Likely qualifying as HSP, if public-facing.

Non-Regulatory Approaches

As with social media platforms, non-regulatory governmental approaches to addressing harms on online gaming platforms and services also exist. The limited and patchwork applicability of legislative frameworks to this sector calls for networks that bring together industry, researchers, policymakers, regulators and others working at the nexus of gaming and issues like extremism, child safety, and gender-based online violence. This section provides an overview of several key non-regulatory and multistakeholder approaches already in place to address these harms.

The European Union Internet Forum (EUIF) was established by the European Commission in 2015 to create a collaborative environment between governments and private sector stakeholders to address illegal content online; it includes online gaming platforms and services.[130] As part of its mission to address online radicalisation, the EUIF held a meeting in October 2021 with tech companies, law enforcement and relevant practitioners. Its focus was "establish[ing] an evidence base on violent extremist use of video gaming and related services and to understand emerging challenges as well as to exchange best practices and develop ideas to address potential challenge".[131]

Notably, the meeting included gaming-adjacent platforms included Twitch, Discord and YouTube. The EUIF has also highlighted the pressing need for more research on the link between gaming and extremism, and called for data transparency.[132]

Australia's independent online safety regulator, the eSafety Commissioner, developed a Safety by Design (SbD) initiative. This voluntary initiative, designed with industry for industry, illustrates how non-regulatory approaches led by government can address online harms through industry uplift. SbD is designed to be flexible and applicable across the online ecosystem, including gaming and gaming-adjacent platforms. It focuses on the ways in which technology companies can minimise online threats by anticipating, detecting and eliminating online harms before they occur.

The SbD principles also promote the technology industry's strengths in innovation; for example, encouraging new thinking and investment to support product development which prioritises online safety.

The SbD principles are also supported by practical tools that help "guide organisations as they embed the rights of users and user safety into the design and functionality of products and services".[133] As technologies and online environments evolve, the Safety by Design approach, alongside Privacy by Design and Security by Design approaches, aims to ensure harms can be mitigated before they occur.

Another non-regulatory approach for government actors to consider is research and evidence building to inform either legislation or other non-regulatory approaches. Such research should ensure that new and emerging harms and vulnerabilities are understood and can be planned for, as technologies and their use changes and adapts. For example, the Swedish Psychological Defence Agency (MPF) is a civil defence agency which aims to identify foreign information campaigns within Sweden and build up Swedish psychological defence.[134]

The MPF also provides research on new domestic trends. In 2023, it noted the high number of Swedish users of online games in a report on FIMI on video game platforms. The report gives detailed threat assessments, threat scenarios and platform-specific vulnerabilities with recommendations to combat online threats.[135] This is a commendable example of government-backed threat identification and evidence-building, especially on an issue area where regulation is difficult to balance with fundamental human rights.

Non-Governmental and Industry Responses

There have also been a variety of non-governmental and industry efforts to investigate how gaming platforms can be exploited by bad actors or cause harm to users, develop recommendations to make the platforms safer, and provide opportunities for relevant stakeholders to communicate.

- The **Extremism and Gaming Research Network (EGRN)** is a non-profit initiative designed to connect researchers, practitioners, policymakers, and the private sector to conduct research at the nexus of gaming and extremism. It also provides training and guidance to gaming stakeholders, including policy-makers, law enforcement, and gamers on how to combat terrorism online globally. It was started by practitioners and researchers who acknowledged that gaming communities "are not generally included in contemporary prevention of targeted violence efforts". This led to a gap in research and prevention programs, as well as a need for a central organisation to design research agendas and distribute research.[136] EGRN also connects expert members and staff with others who may need training and organises workshops. It currently has more than 145 members, including the Global Internet Forum to Counter Terrorism, Tech Against Terrorism and the Royal United Services Institute.

- The **Radicalisation Awareness Network (RAN)** is a coalition of over 6000 frontline practitioners[137] across Europe who work with individuals/populations who are vulnerable to radicalisation or radicalised.[138] RAN aims to bring frontline practitioners together and enable them to share knowledge, experiences and best practices to effectively combat extremism within their communities. To further this mission, RAN holds topical working groups for practitioners and releases publications that integrate research findings and insights from the working groups. Notably, RAN has published several significant reports on the issue of extremism within video game platforms. One such publication is a policy paper developed for a working group that included law enforcement, key practitioners, and representatives from gaming and gaming adjacent companies like Twitch, Discord and Roblox.[139]

Multistakeholder networks that enable gaming companies and platforms to share information, collectively fund research and develop technological solutions are one method that companies have pursued.

- The **Fair Play Alliance** is a coalition of more than 200 gaming companies who are working to make online games more inclusive, aiming towards the creation of games that are free from harassment, discrimination and abuse. More specifically, the Fair Play Alliance created the Disruption and Harms in Online Gaming Framework. This aims to empower game developers, publishers, community managers and the online gaming community with more knowledge and tools to support the development and management of safer online games. The Framework lists the types of harms that exist within an online gaming environment[140] and is an industry-wide shared language and knowledge base.[141] The Fair Play Alliance also holds webinars with relevant researchers and organisations on a wide variety of topics. These include addressing supremacist narratives through game development, responsible gaming (the practice of making sure gaming is used for entertainment rather than gambling purposes) and the UK's Online Safety Act.[142]

- The **Global Internet Forum to Counter Terrorism (GIFCT)** is an NGO "designed to prevent terrorists and violent extremists from exploiting digital platforms". It was founded by Meta, Microsoft, YouTube, and X in 2017.[143] Its membership has since grown to more than 30 organisations, including Discord and Twitch. GIFCT invests in technological solutions, including its hash-sharing database. It also provides communication channels for platforms to share information on breaking incidents, administers a Content Incident Protocol and funds research, primarily through its academic research initiative, the Global Network on Extremism and Technology (GNET).[144] GNET regularly publishes sector-leading research on how extremists use gaming and gaming-adjacent platforms. One such example is "Gaining Steam," which outlines how gaming platforms can be used for far-right radicalisation.[145]

- **Tech Against Terrorism** is a non-profit that conducts threat analysis, facilitates knowledge sharing. It also develops technical tools to disrupt terrorist content online.[146] It does this work through open-source investigation and its own research which informs policy recommendations. Tech Against Terrorism receives funding from tech platforms, GIFCT and various governments. Through its Mentorship Programme, it also partners with the UN Counter-Terrorism Directorate, the Christchurch Call to Action, the EU Internet Forum, the Airbnb Trust and Safety Council and others.[147] Tech Against Terrorism has published research on how extremists use gaming including its annual "State of Play" reports.[148]

- The **Family Online Safety Institute** is a non-profit that conducts research, provides resources, and convenes stakeholders on how to create a safer internet for kids and their families. It currently has more than 30 members, including Discord, Epic Games and Roblox.[149] It publishes research and guides on gaming focused on identifying and mitigating harms to children. These include the Safer Gaming Guide, which collates resources on parental controls, the ESRB ratings guide and tips for protecting children from cyberbullying.[150]

Mitigation Measures

This section reviews some of the possible mitigation measures that could address gaps in design and policies, including:

- Additional content moderation actions,
- Transparency reporting requirements,
- Increased data access for researchers,
- Safety by design (SbD) principles,
- Gamifying prevention principles,
- Better information sharing,
- Industry-wide standards.

Platform Policies

One approach to mitigate harms in gaming and gaming-adjacent platforms is to institute more comprehensive content moderation mechanisms and policies to slow the spread of harmful content. While many gaming and gaming-adjacent platforms have terms of service that prohibit violent or explicit content, they often do not specifically mention terrorist or extremist content, or hate speech.

Even companies which have introduced anti-extremism policies into their terms and conditions (such as Microsoft and Activision Blizzard) do not include propaganda and FIMI in those policies. This content is often harder to detect as it requires knowledge of context, symbolism, coded messages and the ability to recognising motives, which are more difficult to create standards around. Nevertheless, companies should work with external experts to continually update these terms to capture this content.[151]

Platforms can take alternative methods to moderating content that would not require making broad distinctions in general terms of service. These include evaluating flagged accounts' behaviour over time or proactively monitoring higher-risk elements of gaming spaces. For instance, Riot Games considers players' on-platform behaviour over time as part of content moderation and is expanding its ability to detect accounts that receive significantly more reports than others, including for gameplay offenses and inappropriate names.[152]

As mentioned above, many players might not report violative user behaviour because they believe it is an ineffective method for removing players or seeing action from game administrators.[153] This leads to knowledge gaps and subsequently lacklustre enforcement in platforms that rely on reports as a metric for moderation. This means that platforms must make user reporting more accessible, particularly to monitor higher-risk elements of games such as voice communications.[154] Riot Games has also discussed the importance of automated voice evaluation in detecting voice chat abuse.[155] After various versions of the game Call of Duty began using automated voice moderation to address harmful behaviour over voice chat, toxicity decreased by 25 to 50 percent, according to results released by Activision and Modulate.[156]

Platforms could also institute non-punitive and more positive measures to encourage positive play. For instance, they could implement player endorsements, where players can celebrate their teammates and friends. Blizzard implemented this in Overwatch 2 and has revamped endorsements to give them more impact.[157]

Consistent Enforcement of Platform Policies

Regardless, terms of service should be presented in a clear and accessible manner and consistently enforced.[158] Gamification is a particularly suitable feature for innovation to increase user understanding of games. For example, codes of conduct can be incorporated into in-game activities and onboarding processes.[159] Consistent terms of service enforcement are also key to setting expectations of behaviour for players. They can also make it easier for platforms in determining what types of content or certain use cases warrants removal or other punitive measures.[160] Clear punitive measures can also as a deterrent to players, overall lowering the volume and spread of harmful content.[161]

In addition to the platform's own terms of services, they can institute off-service conduct policies, where platforms suspend or ban accounts that have been linked to TVE activities off-platform (e.g., on social media or offline). Twitch implemented a policy for off-service conduct, which explicitly bans individual or organisations who engage in violent extremism, terrorist activities, and sexual exploitation of youth.[162] This can help prevent threat actors that establish a relatively benign presence on gaming platforms to draw users into higher-risk spaces.[163]

Transparency

Ensuring that platform policies are adequate and being fully enforced is only possible with sufficient transparency and data access for external stakeholders, such as researchers, civil society, regulators, and policymakers, to evaluate them.

Few gaming platforms historically have voluntarily published transparency reports. When US Congresswoman Lori Trahan's office reached out to gaming companies last year, she asked about their willingness to voluntarily share certain data in transparency reports and 7 of the 14 companies provided no answer.[164] While some regulation has passed to make meaningful strides in mandating that certain platforms publish transparency reports, such as the EU's Digital Services Act, many smaller gaming platforms are exempt from transparency reporting requirements due to their userbase.

Furthermore, much of the global gaming userbase is not covered by the regulation frameworks reviewed in this brief. Due to this, it is incredibly difficult for researchers, policymakers, and even the platforms themselves to fully understand what harms exist on their platforms and which measures can successfully mitigate them.

Data Access for Researchers

While transparency reports are helpful in providing a snapshot of reported content and how platforms are adhering to their policies, there also needs to be adequate data access for external researchers to ensure platform compliance and accountability, as well as research topics or trends that might not surface in transparency reports. Rosenblatt and Barrett illustrated the lack of data availability when writing, "although the lack of in-game communication data had made it impossible for academic researchers to track the presence of extremists in a systematic way, there is enough anecdotal evidence—including evidence obtained from police investigation files—to infer that in-game chatrooms can and do function as "radicalisation funnels" in at least some cases.[165] To address this, they recommend that gaming and gaming-adjacent companies provide researchers with anonymised data about in-game communication and amend their terms of service to inform players of potential external review while prioritising and maintaining their privacy.[166]

"Current understanding of extremism in gaming spaces draws mostly from gamer surveys and focus groups, in-platform investigative work by journalists and researchers, anecdotal evidence from media accounts, and analysis of police investigation files and other materials related to mass shootings. The empirical study of the misuse of gaming spaces by extremists has been limited by the gaming industry's reluctance to provide researchers with access to the information required to conduct large-scale quantitative studies. "Game companies for the most part don't want to share their data with researchers," Katie Salen, a professor at the University of California at Irvine, noted in an interview. "That is the big challenge."[167]

Implementing Safety by Design Principles and Industry-Wide Standards

Gaming and gaming-adjacent platforms across the online gaming sector often see similar types of violative or harmful content. Therefore, similar standards of safety and risk mitigation should apply across the industry. This can be supported by the industry-wide adoption of shared standards and expectations, such as Safety by Design (SbD). Information sharing between gaming companies and gaming-adjacent platforms about emerging trends and effective mitigation strategies are vital to help identify and combat violative and harmful content across the online gaming ecosystem.

Many companies already participate in information-sharing schemes through membership with organisations such as GIFCT, Tech Against Terrorism, and the Fair Play Alliance. Such organisations provide spaces for companies and developers to share funds, research and house tools, such as hash-sharing databases. They can also serve as useful spaces for companies to work with one another and thematic experts to uplift industry standards by prioritising safety and risk mitigation throughout product lifestyles. For example, this can include empowering gamers through effective reporting mechanisms or incorporating their viewpoints into game policies.[168] These centralised spaces also allow for more diverse perspectives to inform policy or design responses, which is critical to addressing negative aspects of gaming culture.[169]

However, not all gaming or gaming adjacent companies are part of these information-sharing initiatives. For example, only four of GIFCT's members are gaming companies, despite over 200 gaming companies being a part of the Fair Play Alliance and user-generated terrorist and extremist content being present in many games.[170] Increasing the membership of organisations like GIFCT makes it easier to create industry-wide buy-in to close loopholes and create effective policies for addressing extremism on gaming platforms. It also allows the membership organisations to create more stringent safety goals for members and more rigorous assessment schemes.[171]

These efforts will have further impact if they consistently bring in external extremism and terrorism experts, civil society organisations and academics to share up-to-date information and inform more effective mitigation strategies.

Gamifying Prevention Measures

Gaming and gaming-adjacent platforms can utilise the same design elements that appeal to users to facilitate counterprogramming or prosocial programming; this is programming that specifically aims to prevent and counter harms such as extremism, or promote healthier ways to interact with other users. These initiatives can help users identify the signs of radicalisation and build trust with law enforcement or other flaggers.

Experts and developers can create bespoke preventing and countering violent extremism (P/CVE) initiatives that can range from standalone experiences or be created for specific settings, such as schools.[172] P/CVE initiatives can also be gamified using narratives which can appeal to users and make the experience feel more familiar or fun, rather than geared towards education.[173] Gamifying content moderation and other actions that promote prosocial norms can also be effective measures to teach users about how to comply with companies' terms of service and support efforts to remove extremist and terrorist content and hate from platforms.

Experts and officials can also use existing games as a medium to meet, talk and build trust with players. The North Yorkshire Police's Cops vs. Kids and the Dutch Police's Gamen Met De Politie, in which police play games with local children are two examples of this model.[174] Currently most of these efforts involve police, but they could be expanded to other audiences to broaden trust amongst players. For example, this could include setting up initiatives with parents or trusted flaggers who are trained to recognise and share signs of potential radicalisation or other harms in gaming spaces. These efforts could also use gaming aesthetics or gaming culture, such as including popular streamers or influencers in initiatives.

Conclusion

The normalisation of hate and harassment in gaming culture is deeply worrying. In ADL's 2023 survey of multiplayer gamers, an estimated 83 million of the 110 million online gamers in the US were exposed to hate and harassment over a six-month period.[175] Further, the same survey found that three out of four young people (aged 10-17) experience harassment while playing video games. Aside from hate and harassment, online gaming spaces have also been exploited by extremists to propagate and push their ideology on potentially vulnerable gamers.[176]

The growing evidence base illustrates how gaming services and adjacent platforms can present significant risks to children as well as to adult users. This illustrates the need for interventions from government, industry and civil society to ensure online safety in this space. This policy brief set out to review and identify gaps in the evidence base on the nature and extent of risks. It also provides an overview of the current regulatory and non-regulatory approaches and mitigation measures that government and non-governmental stakeholders – including industry – have taken to address these risks.

Reviewing the current evidence base on risks has highlighted the critical role for researchers and the need for data access and comparable information across gaming platforms, including consistent and comparable industry transparency reports. To this point, an overview of new and proposed online safety regulation in the EU, UK, Australia, Canada and the US indicates that in some jurisdictions, some of these needs will likely be addressed as this legislation is implemented over the coming years.

Particularly in the EU and UK, regular industry transparency reporting requirements apply to (most) interactive, user-to-user gaming experiences. This should provide new insights for both regulators and researchers on industry action, and policy levers for accountability for inaction. In fact, several of the mitigation measures outlined in section 8 provide new benchmarks of online safety which should likely apply to online gaming spaces. If implemented correctly, they may ensure rising expectations from users in these markets on what is acceptable regarding online safety experiences in gaming as well. This includes platform policies for online harms and the moderation of this content, the consistent and predictable enforcement of these platform policies.

In Australia, the Safety by Design initiative, coupled with transparency reports facilitated through the BOSE scheme, may provide valuable insights about how government initiatives can promote and encourage industry uplift in improving user safety.

Given that until now many of these mitigation measures have been driven only by civil society, industry initiatives and researchers, the recently introduced legislative frameworks in these markets will provide insights into what legislation for online safety may (or may not) be able to ensure for online gaming spaces. As of now, questions of scope remain. Enforcement, and subsequent challenges and gaps, will surely become evident in the coming years. They should be considered in other proposals, such as those under debate in Canada and the US.

Recognising that not all types of online risks require regulatory responses, both governmental and multistakeholder non-regulatory approaches were also reviewed. Many of these efforts are significant, ongoing forums and spaces setting the agenda for facilitating further research efforts. They have also established networks which enable gaming companies and platforms to share information, collectively fund research, and develop technological solutions.

Annex: Overview of Key Online Regulations

There are various legal frameworks in place across key jurisdictions that touch upon different service providers and aspects of their operations in the digital sphere, which may also affect the gaming industry. Table 3 summarises the most relevant existing regulations in this space and provides an overview of the respective mandates and key provisions.

Law	Mandate & Key Risks Addressed	Relevant Key Provisions
EU Digital Services Act (2022)	The DSA is a horizontal framework that attempts to answer to a wide set of risks to make the online realm safer for EU citizens. It refers to EU and national legislation for determining illegal content and activities but goes beyond that to also curb harmful content and activities. It does so by introducing a funnel system of due diligence obligations (see right side) depending on types of services and their size: 1. **Intermediary services**: • Mere conduit services provide access to communication networks OR transmit user information in them. • Caching services also provide automatic, intermediate and temporary storage of that information to transmit to other users upon request. 2. **Hosting services** store user information upon request. 3. **Online platforms** store and disseminate user information to the public upon request, with some exceptions (Art. 3 (i)), OR allow users to input queries to perform searches. 4. **Very large online platforms & search engines (VLOPSEs)** have over 45 million monthly active users in the EU, a status determined by the European Commission. **Gaming and adjacent platforms and services** may qualify as an intermediary or hosting service, potentially even as platforms, depending on their functions (see Table 2). The DSA introduces a rather **complex enforcement system** of national-level regulators, the Digital Service Coordinators (DSCs), and the European Commission.	The DSA's due diligence obligations depend on service type and size. This also affects which obligations gaming and adjacent services and platforms must adhere to, if they are at all in scope of the DSA (see Table 2). 1. **Intermediary services** are required to: • **Ensure accountability** through platform points of contacts and legal representatives in the EU, and responding to competent authority orders for illegal content. • **Ensure transparency** through public terms and conditions, and annual and standardised transparency reports outlining content moderation practices. 2. **Hosting services'** duties: • **Content moderation**: Maintain notice-and-action mechanisms and provide statements of reasons for restrictions and a possibility to appeal for users. • **Cooperating with authorities**: Inform when suspecting criminal offences. 3. **Online platforms'** duties: • **Content moderation**: Implement suspension processes for repeated misuse. • **Restrictions** on targeted advertising & deceptive design must be adhered to. • **Traceability** of traders must be ensured. • **Protection of minors** must be ensured. 4. **VLOPSEs**' duties: • **Duty of care**: Significant process of systemic risk assessment & mitigation. • **More transparency/checks and balances**: Provisions for data access for researchers via a vetting system and independent audits.

Law	Mandate & Key Risks Addressed	Relevant Key Provisions
EU Terrorist Content Online Regulation (2021)	The TCO regulates one specific online harm: the **dissemination of terrorist content online**. Terrorist content is defined in Art. 2 (7) by referring to the Counter-Terrorism Directive; Extremist content under the threshold of terrorist content is not in scope. The TCO applies to **hosting service providers (HSPs)**, which: • store content at user request; • disseminate the content to the public at user request (“to a potentially unlimited number of persons” (Art. 2(3)). **Gaming and adjacent platforms and services** may qualify as hosting service providers (HSPs, see Table 2). Key **enforcement actors** are primarily member state authorities, while the European Commission collects monitoring results and publishes implementation reports.	**Hosting Service Providers (HSPs)**, which gaming and adjacent platforms and services may qualify as, have a set of duties to adhere to. 1. **Ensure accountability**: Establish a contact point and legal representative. 2. **Ensure transparency**: State the approach towards curbing the spread of terrorist content in terms and conditions and publish annual transparency reports. 3. **Content Moderation**: Remove terrorist content within one hour after receiving a removal order by member state authorities which are binding (though may be scrutinised by host competent authority, also at HSP or user request). Inform users about removals and establish remedies and complaint mechanisms. 4. **Cooperate with authorities**: Inform authorities about removals after orders and preserve content that has been removed or to which access has been disabled for 6 months. Inform competent criminal prosecution authorities when becoming aware of terrorist content constituting an “imminent threat to life”. Moreover, HSPs “exposed to terrorist content” (Art. 5) have additional obligations to fulfil: 1. **Specific measures**: Implement specific measures and report on them once the status of “exposure” is determined by member state authorities. Measures may include adapting personnel, technical capabilities, or user moderation and reporting mechanisms. When applying these, fundamental rights must be taken into account. 2. **More transparency**: Inform in terms and conditions about how terrorist misuse is addressed.

Law	Mandate & Key Risks Addressed	Relevant Key Provisions
UK Online Safety Act (2023)	The UK OSA aims to create a safer online environment by holding platforms accountable for the content they host and the interactions they facilitate. It applies to two types of services: ‟user-to-user services” (or U2U), which includes content that is generated, uploaded and shared by the service users, and ‟search services”, such as web search engines. It places significant duties on these regulated services, to protect users, especially children, from **harmful and illegal content** (see right side). The Act also mandates procedures for protecting users' freedom of expression and privacy. **Online gaming platforms** that enable user-to-user interactions are classified as ‟regulated user-to-user services” under the UK OSA. This classification subjects them to various duties and responsibilities to protect users from harmful and illegal content. The **UK's media regulator, Ofcom**, is tasked with overseeing the implementation of these duties and issuing codes of practice.	The Act includes provisions that are relevant to a wide range of online services, including gaming platforms that allow user-to-user interaction and the sharing of content. Relevant provisions include: 1. **Duties of care**: Regulated services must comply with duties of care related to illegal content, content that is harmful to children, and other harmful content. They are required to assess the risks associated with their services and implement measures to mitigate these risks. 2. **Content moderation**: The Act mandates that regulated services have robust content moderation practices. This includes the ability to report, assess, and remove illegal and harmful content efficiently. 3. **Protection of children**: Specific provisions in the OSA focus on protecting children from harmful content. Regulated services likely to be accessed by children must conduct assessments to identify risks to children and take appropriate measures to safeguard them. 4. **Transparency and reporting**: Regulated services must provide clear processes for users to report harmful content. They also need to maintain transparency reports detailing their efforts to comply with the UK OSA's requirements. 5. **Regulatory oversight**: Regulated services must adhere to Ofcom's codes of practice and may be subject to audits and investigations to ensure compliance.

Law	Mandate & Key Risks Addressed	Relevant Key Provisions
Australian Online Safety Act (2021)	Australia's OSA aims to create a safer online environment for all Australians by holding online platforms accountable for the content they host and the safety of their users. **Gaming platforms** may qualify as online service providers under the Act. Specifically, "relevant electronic services" are within scope, which include "a chat service that enables end-users to communicate with other end-users", and "a service that enable end-users to play online games with other end-users".[177] The Act is overseen by the Australian eSafety Commissioner.	Key provisions include: 1. Basic Online Safety Expectations (BOSE): • Establishes a set of expectations for online service providers (e.g., social media, messaging apps) regarding the safety of users. 2. Removal of harmful content: • The eSafety Commissioner has the authority to issue takedown notices to platforms, requiring the removal of harmful content within specified time frames. 3. Cyberbullying and online abuse protections: • Strengthens protections against cyberbullying, especially for children. 4. Adult Cyber Abuse Scheme: • Extends protections to adults, allowing them to report serious cases of cyber abuse. 5. Abhorrent violent material: • The Act targets the rapid dissemination of abhorrent violent material, such as terrorist acts or extreme violence. 6. Proactive role of the eSafety Commissioner: • The Commissioner is empowered to develop and promote online safety education programs. 7. Enforcement and penalties: • The penalties for non-compliance can be as high as $555,000 AUD for individuals and $11.1 million AUD for corporations. 8. Industry codes and standards: • The Act allows the development of industry codes and standards that online platforms must adhere to. • These codes cover areas such as content moderation, reporting mechanisms, and transparency measures.

Endnotes

1 Wainwright, T. (March 20, 2023). "Ready, player four billion: the rise of video games". The Economist. Retrieved from https://www.economist.com/special-report/2023/03/20/ready-player-four-billion-the-rise-of-video-games Parvini, S. (August 21, 2023). "3 takeaways on the state of the global games market (hint: it's growing)". Los Angeles Times. Retrieved from https://www.latimes.com/entertainment-arts/business/story/2023-08-21/global-gaming-industry-report-2023-league-of-legends-activision-electronic-arts-nintendo-mobile-gaming-mario-bros

2 Anti-Defamation League's Center for Technology and Society. (2022). "Hate is No Game: Hate and Harassment in Online Games 2022". Anti-Defamation League. Retrieved from https://www.adl.org/sites/default/files/documents/2022-12/Hate-and-Harassment-in-Online-Games-120622-v2.pdf; Rosenblat, M.O. and Barett, P.M. (2023). "Gaming The System: How Extremists Exploit Gaming Sites And What Can Be Done To Counter Them". NYU Stern Center for Business and Human Rights. p. 14. Retrieved from https://bhr.stern.nyu.edu/wp-content/uploads/2024/01/NYUCBHRGaming_ONLINEUPDATEDMay16.pdf; Lamphere-Englund, G. & White, J. (2023). "The Online Gaming Ecosystem: Assessing Socialisation, Digital Harms, and Extremism Mitigation Efforts". Global Network on Extremism and Technology (GNET). p. 11. Retrieved from https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf

3 Kowert, R., Martel, A., & Swann, W. B. (2022). "Not just a game: Identity fusion and extremism in gaming cultures". Frontiers in Communication. Retrieved from https://www.frontiersin.org/journals/communication/articles/10.3389/fcomm.2022.1007128/full

4 UN Women. (2023). "Expert Group Meeting report: Technology-facilitated violence against women: Towards a common definition". UN Women. Retrieved from https://www.unwomen.org/en/digital-library/publications/2023/03/expert-group-meeting-report-technologyfacilitated-violence-against-women

5 Bundtzen, Sara. (2023). "Misogynistic Pathways to Radicalisation: Recommended Measures for Platforms to Assess and Mitigate Online Gender-Based Violence". Institute for Strategic Dialogue (ISD). Retrieved from https://www.isdglobal.org/isd-publications/misogynistic-pathways-to-radicalisation-recommended-measures-for-platforms-to-assess-and-mitigate-online-gender-based-violence/

6 Wainwright, T. (2023). "Ready, player four billion: the rise of video games". The Economist. Retrieved from https://www.economist.com/special-report/2023/03/20/ready-player-four-billion-the-rise-of-video-games Parvini, S. (2023). "3 takeaways on the state of the global games market (hint: it's growing)". Los Angeles Times. Retrieved from https://www.latimes.com/entertainment-arts/business/story/2023-08-21/global-gaming-industry-report-2023-league-of-legends-activision-electronic-arts-nintendo-mobile-gaming-mario-bros

7 Ofcom. (March 29, 2023). "Children and Parents: Media Use and Attitudes". Ofcom. Retrieved from https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/childrens-media-use-and-attitudes-2023/childrens-media-use-and-attitudes-report-2023.pdf?v=329412

8 UNICEF. (2024). " Video games can have a positive impact on children – if they are designed right, says new study: New research shows games can be good for children ". UNICEF. Retrieved from https://www.unicef.org/innocenti/press-releases/video-games-can-have-positive-impact-children-if-they-are-designed-right-says-new

9 Crossley, R. (2014). "Mortal Kombat: Violent game that changed video games industry". BBC. Retrieved from https://www.bbc.com/news/technology-27620071

10 E.g., Sherry, J. (2001). "The effects of violent video games on aggression: a meta-analysis". Human Communication Research. 27(3): 409–431. Retrieved from https://academic.oup.com/hcr/article-abstract/27/3/409/4554758?redirectedFrom=fulltext&login=false found an effect of violent video games on aggression levels yet smaller than the one caused by violent television. Ferguson, Christopher J., Kilburn, J. (2009). "The public health risks of media violence: a meta-analytic review". The Journal of Pediatrics. 154 (5): 759–763. Retrieved from https://doi.org/10.1016%2Fj.jpeds.2008.11.033 did not find such an effect.

11 Crossley, R. (June 2, 2014). "Mortal Kombat: Violent game that changed video games industry". BBC. Retrieved from https://www.bbc.com/news/technology-27620071

12 Romano, A. (January 7, 2021). "What we still haven't learned from Gamergate". Vox. Retrieved from https://www.vox.com/culture/2020/1/20/20808875/gamergate-lessons-cultural-impact-changes-harassment-laws

13 Lamphere-Englund, G. & White, J. (May 2023). "The Online Gaming Ecosystem: Assessing Digital Socialisation, Extremism Risks and Harms Mitigation Efforts". Global Network on Extremism & Technology (GNET). Retrieved from https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf

14 Ibid.

[15] Kowert R., Martel A. and Swann W.B. (2022). ”Not just a game: Identity fusion and extremism in gaming cultures”. Front. Commun. Retrieved from https://www.frontiersin.org/journals/communication/articles/10.3389/fcomm.2022.1007128/full

[16] E.g., Lamphere-Englund, G. & White, J. (May 2023) ”The Online Gaming Ecosystem: Assessing Digital Socialisation, Extremism Risks and Harms Mitigation Efforts‟. Global Network on Extremism & Technology (GNET). Retrieved from https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf; Pamment, J., Falkheimer, J., & Isaksson, E. (2023). ”Malign Foreign Interference and Information Influence on Video Game Platforms: Understanding the Adversarial Playbook”. MPF report series 3/2023, Psychological Defence Research Institute, Lund University. Retrieved from https://www.mpf.se/en/2023/10/09/malign-foreign-interference-and-information-influence-on-video-game-platforms-understanding-the-adversarial-playbook-2/

[17] For example, Roblox is frequently understood as a gaming platform rather than a game itself as it allows players to build and engage in their own mini games. Garrett, U. (August 11, 2023). “What is Roblox? Here’s everything you need to know”. CNN. Retrieved from https://edition.cnn.com/cnn-underscored/electronics/what-is-roblox

[18] Ofcom (2024). “Protecting people from illegal harms online. Volume 2: The causes and impacts of online harm. Consultation”, p. 20. Ofcom. Retrieved from https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/270826-consultation-protecting-people-from-illegal-content-online/associated-documents/volume-2-the-causes-and-impacts-of-online-harm/?v=330417

[19] Lamphere-Englund, G. & White, J. (May 2023). “The Online Gaming Ecosystem: Assessing Socialisation, Digital Harms, and Extremism Mitigation Efforts”. Global Network on Extremism and Technology (GNET). Retrieved from https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf

[20] Ofcom. (2024). ”Protecting people from illegal harms online. Volume 2: The causes and impacts of online harm. Consultation”. Ofcom. Retrieved from https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/270826-consultation-protecting-people-from-illegal-content-online/associated-documents/volume-2-the-causes-and-impacts-of-online-harm/?v=330417

[21] ISD Germany & HateAid (March 9, 2022). „Hass als Berufsrisiko: Digitale Gewalt und Sexismus im Bundestagswahlkampf‟. ISD Germany & HateAid. Retrieved from https://www.isdglobal.org/isd-publications/hass-als-berufsrisiko-digitale-gewalt-und-sexismus-im-bundestagswahlkampf/

[22] Kilmer, E. and Kowert, R. (2024). “Empowering The Gaming Industry: Strategies for Addressing Hate, Harassment, and Extremism in Online Communities”. Take This. Retrieved from https://www.takethis.org/2024/02/empowering-industry-whitepaper/

[23] Anti-Defamation League’s Center for Technology and Society (June 2, 2024). “Hate is No Game: Hate and Harassment in Online Games 2023”. Anti-Defamation League. Retrieved from https://www.adl.org/resources/report/hate-no-game-hate-and-harassment-online-games-2023

[24] Kilmer, E. and Kowert, R. (2024). “Empowering The Gaming Industry: Strategies for Addressing Hate, Harassment, and Extremism in Online Communities”. Take This. Retrieved from https://www.takethis.org/2024/02/empowering-industry-whitepaper/

[25] Anti-Defamation League. (2022). “Online Hate and Harassment: The American Experience 2022”. Anti-Defamation League. Retrieved from https://www.adl.org/resources/report/online-hate-and-harassment-american-experience-2022

[26] Anti-Defamation League’s Center for Technology and Society (2024). ”Hate is No Game: Hate and Harassment in Online Games 2023”. Anti-Defamation League. Retrieved from https://www.adl.org/resources/report/hate-no-game-hate-and-harassment-online-games-2023

[27] Bryter Research. (2023). “Women Gamers Report”. Bryter Research. Retrieved from https://www.bryter-global.com/women-gamers-report-2023

[28] Ibid.

[29] Ibid.

[30] Yokoi, T. (2021). “Female Gamers Are On The Rise. Can The Gaming Industry Catch Up?”. Forbes. Retrieved from https://www.forbes.com/sites/tomokoyokoi/2021/03/04/female-gamers-are-on-the-rise-can-the-gaming-industry-catch-up/?sh=1767f1e6f9fe

[31] Lamphere-Englund, G. & White, J. (May 2023) The Online Gaming Ecosystem: Assessing Digital Socialisation, Extremism Risks and Harms Mitigation Efforts. Global Network on Extremism & Technology (GNET). Retrieved from https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf

[32] Taylor, Mark. (2022). ”UK Games Industry Census 2022”. Ukie. Retrieved from https://ukie.org.uk/resources/uk-games-industry-census-2022

[33] Bryter Research. (2023). "Women Gamers Report". Bryter Research.
Retrieved from https://www.bryter-global.com/women-gamers-report-2023

[34] Anti-Defamation League's Center for Technology and Society (2024). "Hate is No Game: Hate and Harassment in Online Games 2023". Anti-Defamation League. Retrieved from https://www.adl.org/resources/report/hate-no-game-hate-and-harassment-online-games-2023; After the October 7th terrorist attack in Israel, a global rise in antisemitic incidents have been recorded. However, there has yet to be a comprehensive study on the attack's impact on harassment on video game platforms.
Retuers. (2023). "How the surge in antisemitism is affecting countries around the world". Reuters.
Retrieved from https://www.reuters.com/world/how-surge-antisemitism-is-affecting-countries-around-world-2023-10-31/

[35] Lamphere-Englund, G. & White, J. (2023). "The Online Gaming Ecosystem: Assessing Digital Socialisation, Extremism Risks and Harms Mitigation Efforts". Global Network on Extremism & Technology (GNET).
Retrieved from https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf

[36] Romano, A. (2021). "What we still haven't learned from Gamergate". Vox.
Retrieved from https://www.vox.com/culture/2020/1/20/20808875/gamergate-lessons-cultural-impact-changes-harassment-laws

[37] Lamphere-Englund, G. & White, J. (2023). "The Online Gaming Ecosystem: Assessing Socialisation, Digital Harms, and Extremism Mitigation Efforts". Global Network on Extremism and Technology (GNET).
Retrieved from https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf

[38] France 24. (2018). "New Hezbollah video game lets players annihilate IS fighters in Syria". France 24.
Retrieved from https://www.france24.com/en/20180301-hezbollah-video-game-syria-lebanon

[39] Lamphere-Englund, G. & White, J. (2023). "The Online Gaming Ecosystem: Assessing Socialisation, Digital Harms, and Extremism Mitigation Efforts". Global Network on Extremism and Technology (GNET).
Retrieved from https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf

[40] Rosenblat, M.O. and Barett, P.M. (2023). "Gaming The System: How Extremists Exploit Gaming Sites And What Can Be Done To Counter Them". NYU Stern Center for Business and Human Rights.
Retrieved from https://bhr.stern.nyu.edu/wp-content/uploads/2024/01/NYUCBHRGaming_ONLINEUPDATEDMay16.pdf

[41] Lamphere-Englund, G. & White, J. (2023). "The Online Gaming Ecosystem: Assessing Socialisation, Digital Harms, and Extremism Mitigation Efforts". Global Network on Extremism and Technology (GNET).
Retrieved from https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf

[42] Rosenblat, M.O. and Barett, P.M. (2023). "Gaming The System: How Extremists Exploit Gaming Sites And What Can Be Done To Counter Them". NYU Stern Center for Business and Human Rights.
Retrieved from https://bhr.stern.nyu.edu/wp-content/uploads/2024/01/NYUCBHRGaming_ONLINEUPDATEDMay16.pdf

[43] Ibid; Anti-Defamation League. (n.d.). "88". Anti-Defamation League. Retrieved from https://www.adl.org/resources/hate-symbol/88

[44] Rosenblat, M.O. and Barett, P.M. (2023). "Gaming The System: How Extremists Exploit Gaming Sites And What Can Be Done To Counter Them". NYU Stern Center for Business and Human Rights.
Retrieved from https://bhr.stern.nyu.edu/wp-content/uploads/2024/01/NYUCBHRGaming_ONLINEUPDATEDMay16.pdf

[45] Davey, Jacob. (2021). "Gamers who Hate: An Introduction to ISD's Gaming and Extremism Series". Institute for Strategic Dialogue.
Retrieved from https://www.isdglobal.org/wp-content/uploads/2021/09/20210910-gaming-reportintro.pdf

[46] Gais, H and Edison Hayden, Michael. (2020). "Extremists Are Cashing in on a Youth-Targeted Gaming Website." Southern Poverty Law Center. Retrieved from https://www.splcenter.org/hatewatch/2020/11/17/extremists-are-cashing-youth-targeted-gaming-website

[47] Ibid.

[48] D'Anastasio, C. (2021). "A Game Livestreaming Site Has Become an Extremist Haven" Wired.
Retrieved from https://www.wired.com/story/dlive-livestreaming-site-extremist-haven/

[49] Thomas, Elise. (2021). "The Extreme Right on DLive". Institute for Strategic Dialogue.
Retrieved from https://www.isdglobal.org/wp-content/uploads/2021/08/03-gaming-report-dlive-1.pdf

[50] Wiegold, L., Winkler, C., & Jaskowski, J. (2024). "Camera, Action, Play: An Exploration of Extremist Activity on Video- and Livestreaming Platforms". Global Network on Extremist & Technology. Retrieved from https://gnet-research.org/2024/07/18/camera-action-play-an-exploration-of-extremist-activity-on-video-and-livestreaming-platforms/

[51] Ibid.

[52] Pamment, J., Falkheimer, J., & Isaksson, E. (2023). ”Malign Foreign Interference and Information Influence on Video Game Platforms: Understanding the Adversarial Playbook”. Psychological Defence Research Institute, Lund University. Retrieved from https://www.mpf.se/en/2023/10/09/malign-foreign-interference-and-information-influence-on-video-game-platforms-understanding-the-adversarial-playbook-2/

[53] Bellingcat (2017). ”The Russian Ministry of Defence Publishes Screenshots of Computer Games as Evidence of US Collusion with ISIS“. Bellingcat. Retrieved from https://www.bellingcat.com/news/mena/2017/11/14/russian-ministry-defence-publishes-screenshots-computer-games-evidence-us-collusion-isis/

[54] Tencent, owner of Chinese WhatsApp equivalent WeChat, is very active in mobile gaming and is now the corporation with the highest turnover in gaming worldwide – long before Sony, Apple, or Nintendo. The tech giant owns studios that produce mobile versions of in-demand games such as Call of Duty and has acquired stakes in several major studios, including Fortnite’s Epic Games and the entirety of League of Legends’ Riot Games. Brinkhof, T. (2024). “Video Games Are China’s Next Soft Power Grab”. New Lines Magazine. Retrieved from https://newlinesmag.com/spotlight/video-games-are-chinas-next-soft-power-grab/
Moreover, China is increasingly exporting its own games. From the globally popular mobile game “Genshin Impact” to the upcoming expected blockbuster “Black Myth: Wukong” with enhanced narrative and “promoted by Chinese state propaganda”, New Lines Magazine deems this as acts of disseminating Chinese stories of culture and history under the Chinese Communist Party’s (CCP) planned national rejuvenation. The CCP is said to influence the national gaming industry through a permit-based system for developers and exercises censorship over games, including automatic asterisks whenever sensitive issues such as the Tiananmen Square massacre are mentioned in chat. Böhm, M. (2022). “Tencents teure Wetten aufs nächste große Gaming-Phänomen”. DER SPIEGEL. Retrieved from https://www.spiegel.de/netzwelt/web/tencent-das-treibt-den-gaming-giganten-bei-seinen-zahlreichen-investments-an-a-f0371b7a-c5e5-4b4e-bb20-76e1e9eba3f5

[55] Pamment, J., Falkheimer, J., & Isaksson, E. (2023). ”Malign Foreign Interference and Information Influence on Video Game Platforms: Understanding the Adversarial Playbook”. Psychological Defence Research Institute, Lund University. Retrieved from https://www.mpf.se/en/2023/10/09/malign-foreign-interference-and-information-influence-on-video-game-platforms-understanding-the-adversarial-playbook-2/

[56] Gilbert, David. (2024). “DOJ: Russia Aimed Propaganda at Gamers, Minorities to Swing 2024 Election”. Wired. Retrieved from https://www.wired.com/story/project-good-old-usa-russia-2024-election/

[57] Ibid.

[58] Kowert, Rachel, Elizabeth Kilmer, and Alex Newhouse. (2024). ”Culturally justified hate: Prevalence and mental health impact of dark participation in games”. Hawaii International Conference on System Sciences. Retrieved from https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/ad85c3c9-5a16-426d-a694-71f426d9fd18/content

[59] GIFCT Transparency Working Group. (2023). ”Pathways to Meaningful Transparency”. GIFCT. Retrieved fromhttps://gifct.org/wp-content/uploads/2023/09/GIFCT-23WG-0823-Transparency-1.1.pdf

[60] GIFCT Transparency Working Group. (2023). ”Pathways to Meaningful Transparency”. GIFCT. Retrieved fromhttps://gifct.org/wp-content/uploads/2023/09/GIFCT-23WG-0823-Transparency-1.1.pdf

[61] Lamphere-Englund, Galen and Jessica White. (2023). ”The Online Gaming Ecosystem: Assessing Digital Socialisation, Extremism Risks and Harms Mitigation Efforts”. Extremism and Gaming Research Network. Retrieved from https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf

[62] Kowert, Rachel, Elizabeth Kilmer, and Alex Newhouse. (2024). ”Culturally justified hate: Prevalence and mental health impact of dark participation in games”. Hawaii International Conference on System Sciences. Retrieved from https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/ad85c3c9-5a16-426d-a694-71f426d9fd18/content

[63] Kowert, Rachel, Elizabeth Kilmer, and Alex Newhouse. (2024). ”Culturally justified hate: Prevalence and mental health impact of dark participation in games”. Hawaii International Conference on System Sciences. Retrieved from https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/ad85c3c9-5a16-426d-a694-71f426d9fd18/content

[64] Pamment, J., Falkheimer, J., & Isaksson, E. (2023). ”Malign foreign interference and information influence on video game platforms: understanding the adversarial playbook”. Swedish Psychological Defence Agency. Retrieved from https://mpf.se/psychological-defence-agency/about-us/news/2023/2023-10-09-malign-foreign-interference-and-information-influence-on-video-game-platforms-understanding-the-adversarial-playbook; EU Counter-Terrorism Coordinator. (2020). ”Online gaming in the context of the fight against terrorism”. EU Counter-Terrorism Coordinator. Retrieved from https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf

[65] Rosenblatt & Barrett. (2024). ”Gaming The System: How Extremists Exploit Gaming Sites and What Can Be Done to Counter Them”. NYU Stern Center for Business and Human Rights. Retrieved from https://bhr.stern.nyu.edu/wp-content/uploads/2024/01/NYUCBHRGaming_ONLINEUPDATEDMay16.pdf

[66] EU Counter-Terrorism Coordinator. (2020). ”Online gaming in the context of the fight against terrorism‟. EU Counter-Terrorism Coordinator. Retrieved from https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf

[67] Rosenblatt & Barrett. (2024). ”Gaming The System: How Extremists Exploit Gaming Sites and What Can Be Done to Counter Them”. NYU Stern Center for Business and Human Rights. Retrieved from https://bhr.stern.nyu.edu/wp-content/uploads/2024/01/NYUCBHRGaming_ONLINEUPDATEDMay16.pdf

[68] Ibid.

[69] Winkler, C. & Wiegold., L. (2024). ”Gaming the System: The Use of Gaming-Adjacent Communication, Game and Mod Platforms by Extremist Actors”. Global Network on Extremism and Technology. Retrieved from https://gnet-research.org/2024/06/10/gaming-the-system-the-use-of-gaming-adjacent-communication-game-and-mod-platforms-by-extremist-actors/

[70] Rosenblat & Barrett. (2024). ”Gaming The System: How Extremists Exploit Gaming Sites and What Can Be Done to Counter Them”. NYU Stern Center for Business and Human Rights. Retrieved from https://bhr.stern.nyu.edu/wp-content/uploads/2024/01/NYUCBHRGaming_ONLINEUPDATEDMay16.pdf

[71] Miller, C., & Silva, S. (2021). ”Extremists using video-game chats to spread hate‟. BBC. Retrieved from https://www.bbc.com/news/technology-58600181; The West Australian. (2022). ”Roblox: Nazi Germany re-creation discovered in online gaming platform by young Jewish girl from Melbourne”. The West Australian. Retrieved from https://thewest.com.au/technology/gaming/roblox-nazi-germany-re-creation-discovered-in-online-gaming-platform-by-young-jewish-girl-from-melbourne-c-8637499; Singapore Ministry of Home Affairs. (2023). ”Issuance of Orders Under the Internal Security Act Against Two Self-Radicalised Singapore Youths”. Singapore Ministry of Home Affairs. Retrieved from https://www.mha.gov.sg/mediaroom/press-releases/issuance-of-orders-under-the-internal-security-act-against-two-self-radicalised-singaporean-youths/

[72] Lamphere-Englund, G., & White, J. (2023). ”The Online Gaming Ecosystem: Assessing Digital Socialisation, Extremism Risks and Harms Mitigation Efforts”. Global Network on Extremism and Technology. Retrieved from https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf

[73] Pamment, J., Falkheimer, J., & Isaksson, E. (2023). ”Malign foreign interference and information influence on video game platforms: understanding the adversarial playbook”. Swedish Psychological Defence Agency. Retrieved from https://mpf.se/psychological-defence-agency/about-us/news/2023/2023-10-09-malign-foreign-interference-and-information-influence-on-video-game-platforms-understanding-the-adversarial-playbook

[74] Wells, G., et al. (2024). ”Right-Wing Extremism in Mainstream Games: A Review of the Literature”. Games and Culture. Retrieved from https://journals.sagepub.com/doi/full/10.1177/15554120231167214; Pamment, J., Falkheimer, J., & Isaksson, E. (2023). ”Malign foreign interference and information influence on video game platforms: understanding the adversarial playbook”. Swedish Psychological Defence Agency. Retrieved from https://mpf.se/psychological-defence-agency/about-us/news/2023/2023-10-09-malign-foreign-interference-and-information-influence-on-video-game-platforms-understanding-the-adversarial-playbook

[75] Rosenblat & Barrett. (2024). ”Gaming The System: How Extremists Exploit Gaming Sites and What Can Be Done to Counter Them”. NYU Stern Center for Business and Human Rights. Retrieved from https://bhr.stern.nyu.edu/wp-content/uploads/2024/01/NYUCBHRGaming_ONLINEUPDATEDMay16.pdf

[76] Lakhani, S. (2021). ”Video Gaming and (Violent) Extremism: An exploration of the current landscape, trends, and threats”. European Commission. Retrieved from https://home-affairs.ec.europa.eu/document/download/67db2a03-5b45-44f2-b0e9-3b0544a08dfc_en

[77] Lamphere-Englund, G., & White, J. (2023). “The Online Gaming Ecosystem: Assessing Digital Socialisation, Extremism Risks and Harms Mitigation Efforts”. Global Network on Extremism and Technology. Retrieved from https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf

[78] Wells, G., Romhanyi, A., Reitman, J. G., Gardner, R., Squire, K., & Steinkuehler, C. (2024). ”Right-Wing Extremism in Mainstream Games: A Review of the Literature”. Games and Culture. Retrieved from https://doi.org/10.1177/15554120231167214

[79] Activision. (2023). “Call of Duty Voice Chat Moderation FAQ”. Activision. Retrieved from https://support.activision.com/articles/call-of-duty-voice-chat-moderation

[80] EU Counter-Terrorism Coordinator. (2020). ”Online gaming in the context of the fight against terrorism”. EU Counter-Terrorism Coordinator. Retrieved from https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf

81 Lakhani, S. (2021). ”Video Gaming and (Violent) Extremism: An exploration of the current landscape, trends, and threats”. European Commission. Retrieved from https://home-affairs.ec.europa.eu/document/download/67db2a03-5b45-44f2-b0e9-3b0544a08dfc_en

82 EU Counter-Terrorism Coordinator. (2020). ”Online gaming in the context of the fight against terrorism”. EU Counter-Terrorism Coordinator. Retrieved from https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf; Pamment, J., Falkheimer, J., & Isaksson, E. (2023). ”Malign foreign interference and information influence on video game platforms: understanding the adversarial playbook”. Swedish Psychological Defence Agency. Retrieved from https://www.mpf.se/en/2023/10/09/malign-foreign-interference-and-information-influence-on-video-game-platforms-understanding-the-adversarial-playbook-2/

83 Wells, G., Romhanyi, A., Reitman, J. G., Gardner, R., Squire, K., & Steinkuehler, C. (2024). ”Right-Wing Extremism in Mainstream Games: A Review of the Literature”. Games and Culture. Retrieved from https://doi.org/10.1177/15554120231167214

84 Jones, T. (2023). ”Roblox Filter for Parents: Why Kids Want to Bypass Roblox Filter and How?” Famisafe. Retrieved from https://famisafe.wondershare.com/parental-control/how-to-enable-or-bypass-roblox-filter.html

85 Wood, Stuart. (2023). ”Exploring the awareness and usage of parental controls to support digital safety”. Internet Matters. Retrieved from https://www.internetmatters.org/hub/research/research-tracker-awareness-usage-parental-controls/

86 Ministry of Digital Development and Information. (2024). ”MCI’s Survey Suggests Low Awareness among Parents on Child’s Online Gaming Activities”. Ministry of Digital Development and Information. Retrieved from https://www.mddi.gov.sg/media-centre/press-releases/survey-on-childs-online-gaming-activities/

87 Pamment, J., Falkheimer, J., & Isaksson, E. (2023). ”Malign Foreign Interference and Information Influence on Video Game Platforms: Understanding the Adversarial Playbook”. Swedish Psychological Defence Agency. Retrieved from https://www.mpf.se/en/2023/10/09/malign-foreign-interference-and-information-influence-on-video-game-platforms-understanding-the-adversarial-playbook-2/

88 EU Counter-Terrorism Coordinator. (2020). ”Online gaming in the context of the fight against terrorism”. EU Counter-Terrorism Coordinator. Retrieved from https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf

89 House of Commons. (2019). ”Immersive and addictive technologies”. House of Commons Digital, Culture, Media and Sport Committee. Retrieved from https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1846/1846.pdf#page=31

90 Rockloff, M., Russel, A., Greer, N., Lole, L., Hing, N., & Browne, M. (2020). ‟Loot Boxes: Are they grooming youth for gambling?” Central Queensland University. Retrieved from https://www.gambleaware.nsw.gov.au/-/media/loot-boxes---are-they-grooming-youth-for-gambling.ashx?rev=a46de33a110042c3bb809c40cbcc5aa6&hash=0CB3A023D880128604EAB02FA2B06594

91 House of Commons. (2019). ”Immersive and addictive technologies”. House of Commons Digital, Culture, Media and Sport Committee. Retrieved from https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1846/1846.pdf#page=31

92 EU Counter-Terrorism Coordinator. (2020). ”Online gaming in the context of the fight against terrorism‟. EU Counter-Terrorism Coordinator. Retrieved from https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf

93 Lamphere-Englund, G., & White, J. (May 2023). The Online Gaming Ecosystem: Assessing Digital Socialisation, Extremism Risks and Harms Mitigation Efforts. Global Network on Extremism and Technology. https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf

94 Pamment, J., Falkheimer, J., & Isaksson, E. (2023). ”Malign Foreign Interference and Information Influence on Video Game Platforms: Understanding the Adversarial Playbook”. Swedish Psychological Defence Agency. Retrieved from https://www.mpf.se/en/2023/10/09/malign-foreign-interference-and-information-influence-on-video-game-platforms-understanding-the-adversarial-playbook-2/

95 EU Counter-Terrorism Coordinator. (2020). ”Online gaming in the context of the fight against terrorism”. EU Counter-Terrorism Coordinator. Retrieved from https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf

96 Makuch, B. (2019). ”Congressman Shames Blizzard for Letting Nazis Run Wild in ‘World of Warcraft’‟. VICE. Retrieved from https://www.vice.com/en/article/3kxw4b/congressman-lou-correa-shames-blizzard-for-letting-nazis-run-wild-in-world-of-warcraft

97 Schlegel, L. (2020). ”Jumanji Extremism? How games and gamification could facilitate radicalization processes”. Journal for Deradicalisation. Retrieved from https://journals.sfu.ca/jd/index.php/jd/article/view/359

98 Ibid.

99 Kowert, Rachel, Alexi Martel, and William B. Swann. (2022). ‟Not just a game: Identity fusion and extremism in gaming cultures”. Frontiers in Communication. Retrieved from https://www.frontiersin.org/journals/communication/articles/10.3389/fcomm.2022.1007128/full

100 Kowert, Rachel, Alexi Martel, and William B. Swann. (2022).
‟Not just a game: Identity fusion and extremism in gaming cultures”. Frontiers in Communication.
Retrieved from https://www.frontiersin.org/journals/communication/articles/10.3389/fcomm.2022.1007128/full

101 Associated Press. (1982). ‟Around the Nation: Surgeon General Sees Danger in Video Games”. The New York Times. Retrieved from https://www.nytimes.com/1982/11/10/us/around-the-nation-surgeon-general-sees-danger-in-video-games.html

102 Andrews, E, (December 9, 1993). Industry Set to Issue Video Game Ratings as Complaints Rise. The New York Times.
https://www.nytimes.com/1993/12/09/business/industry-set-to-issue-video-game-ratings-as-complaints-rise.html

103 Bajda, P. (2017). ”How Mortal Kombat made the games industry play politics‟. Vice.
Retrieved from https://www.vice.com/en/article/3kawp3/how-mortal-kombat-made-the-games-industry-play-politics

104 European Commission, Directorate-General for Communications Networks, Content and Technology. (2023). ”Understanding the value of a European video games society – Final report”. Publications Office of the European Union. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/075b8bbe-6bd5-11ee-9220-01aa75ed71a1/language-en/format-PDF/source-338004776

105 Dreßler, A. (2023). ”Die EU nimmt sich digitale Riesen vor: Auch große Gaming-Plattformen betroffen?” PC Games.
Retrieved from https://www.pcgames.de/Politik-Thema-237122/Specials/EU-dsa-dma-meta-x-twitter-facebook-tiktok-youtube-gatekeeper-vlop-1432510/

106 European Commission, Directorate-General for Communications Networks, Content and Technology. (2023). ”Understanding the value of a European video games society – Final report‟. Publications Office of the European Union. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/075b8bbe-6bd5-11ee-9220-01aa75ed71a1/language-en/format-PDF/source-338004776

107 Ng, George. (2024). ”Navigating The Digital Services Act: A Guide for Game Developers‟. Forbes. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2024/01/25/navigating-the-digital-services-act-a-guide-for-game-developers/

108 Ibid.

109 Ibid.

110 The OSA applies to two types of services: ‟user-to-user services” (or U2U), which includes content that is generated, uploaded and shared by the service users, and ‟search services”, such as web search engines. Depending on the categorisation of the regulated service, providers have obligations placed on them relating to risk assessments, transparency and accountability measures regarding illegal and harmful content.

111 Ofcom (2024). ‟Protecting people from illegal harms online. Volume 2: The causes and impacts of online harm. Consultation”, p. 20. Ofcom. Retrieved from https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/270826-consultation-protecting-people-from-illegal-content-online/associated-documents/volume-2-the-causes-and-impacts-of-online-harm/?v=330417

112 Ofcom (2024). ‟Protecting people from illegal harms online. Volume 2: The causes and impacts of online harm. Consultation”, p. 20. Ofcom. Retrieved from https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/270826-consultation-protecting-people-from-illegal-content-online/associated-documents/volume-2-the-causes-and-impacts-of-online-harm/?v=330417

113 Australia. (2021). ‟Online Safety Act 2021, No. 76, 2021, Compilation No. 1”. Australia.
Retrieved from: https://www.legislation.gov.au/C2021A00076/latest/text

114 Totilo, Stephen. (2023). ”Exclusive: U.S. rep mulls legislative action to press games industry on extremism”. Axios.
Retrieved from https://www.axios.com/2023/03/02/lori-trahan-games-industry-online-extremism-congress

115 US Congress. (2023). ”Kids Online Safety Act”. US Congress.
Retrieved from https://www.congress.gov/bill/118th-congress/senate-bill/1409/text

116 the process by which a US congressional committee or state legislative session debates, amends, and rewrites proposed legislation

117 Perrino, John. ”What's Different About the US House Version of the Kids Online Safety Act?”, Tech Policy Press.
https://www.techpolicy.press/whats-different-about-the-us-house-version-of-the-kids-online-safety-act/

118 Information Commissioner's Office. (n.d.) ”Introduction to the Children's code”. Information Commissioner's Office.
Retrieved from https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/

[119] State of California. (2022). ”AB-2273 The California Age-Appropriate Design Code Act”. California Legislative Information. Retrieved from https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false

[120] Chavez, Krista. (2022). ”NetChoice Sues California to Protect Families & Free Speech Online”. NetChoice. Retrieved from https://netchoice.org/netchoice-sues-california-to-protect-families-free-speech-online/

[121] Lima-Strong, Cristiano. (2024). “Federal court upholds block on California child online safety law”. Washington Post. Retrieved at https://www.washingtonpost.com/technology/2024/08/16/child-online-safety-california-blocked/

[122] House of Commons of Canada. (2024). ”Bill C-63: An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential and related amendments to other Acts”. House of Commons of Canada. Retrieved from https://www.parl.ca/Content/Bills/441/Government/C-63/C-63_1/C-63_1.PDF

[123] House of Commons of Canada. (2024). ”Bill C-63: An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential and related amendments to other Acts”. House of Commons of Canada. Retrieved from https://www.parl.ca/Content/Bills/441/Government/C-63/C-63_1/C-63_1.PDF

[124] European Union. (2021, 29 April). “Regulation (EU) 2021/784 of the European Parliament and of the Council on addressing the dissemination of terrorist content online”. Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32021R0784

[125] Twitch. (2023). ”EU Terrorist Content Online Regulation 2023 Transparency Report”. Twitch. Retrieved from https://safety.twitch.tv/s/article/2023-EU-Terrorist-Content-Transparency-Report?language=en_US; Roblox. (2024). ”EU Terrorist Content Online Transparency Report 2024”. Roblox. Retrieved from https://corp.roblox.com/wp-content/assets/pdfs/2024_TCO_Report.pdf

[126] Unity. (2024). “Digital Services Act – Compliance Update”. Unity. Retrieved from https://unity.com/de/legal/digital-services-act: “If you offer your services in the EU, such as shipping a game with players in EU regions, you may have obligations”.

[127] Ibid.

[128] Twitch. (2024). “Digital Services Act Information”. Twitch. Retrieved from https://safety.twitch.tv/s/article/Digital-Services-Act-Information?language=en_US

[129] https://safety.twitch.tv/s/article/2023-EU-Terrorist-Content-Transparency-Report?language=en_US

[130] European Commission. (2024). “European Union Internet Forum (EUIF)”. European Commission. Retrieved from https://home-affairs.ec.europa.eu/networks/european-union-internet-forum-euif_en

[131] European Commission. (2021). “EU Internet Forum Misuse of Video-Gaming by Violent Extremists”. European Commission. Retrieved from https://home-affairs.ec.europa.eu/document/download/8ffed0a3-eebd-4396-9acd-47d2be4a9346_en?filename=EUIF%20Technical%20Meeting%20on%20Video%20Gaming%20October%202021%20agenda_en.pdf

[132] Lakhani, S. (2021). “Video Gaming and (Violent) Extremism: An exploration of the current landscape, trends, and threats”. Radicalisation Awareness Network. Retrieved from https://home-affairs.ec.europa.eu/system/files/2022-02/EUIF%20Technical%20Meeting%20on%20Video%20Gaming%20October%202021%20RAN%20Policy%20Support%20paper_en.pdf

[133] eSafety Commissioner. (2019) “Safety by Design Overview”. eSafety Commissioner. Retrieved from https://www.esafety.gov.au/sites/default/files/2019-10/SBD%20-%20Overview%20May19.pdf?v=1724398901443#:~:text=The%20SbD%20Framework%20is%20the%20broad%20program%20of,all%20resources%2C%20have%20SbD%20Principles%20at%20their%20core.

[134] Psychological Defence Agency. (n.d.). “Our Mission”. Psychological Defence Agency. Retrieved from https://www.mpf.se/psychological-defence-agency/about-us/our-mission

[135] Falkheimer, J, Isaksson, E, & Pamment, J. (2023). “Malign foreign interference and information influence on video game platforms: Understanding the adversarial playbook”. Psychological Defence Agency. Retrieved from https://www.mpf.se/psychological-defence-agency/publications/archive/2023-12-01-malign-foreign-interference-and-information-influence-on-video-game-platforms-understanding-the-adversarial-playbook

[136] Extremism and Gaming Research Network. (n.d.) ”About Us”. Extremism and Gaming Research Network. Retrieved from https://extremismandgaming.org/about/

[137] European Council. (n.d.) ”EU measures to prevent radicalisation”. European Council. Retrieved from https://www.consilium.europa.eu/en/policies/fight-against-terrorism/preventing-radicalisation/

138 European Commission. (n.d.) ”About RAN Practitioners”. European Commission. Retrieved from https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/about-ran_en

139 European Commission. (2021.) ”EU Internet Forum Misuse of Video-Gaming by Violent Extremists”. European Commission. Retrieved from https://home-affairs.ec.europa.eu/system/files/2022-02/EUIF%20Technical%20Meeting%20on%20Video%20Gaming%20October%202021%20agenda_en.pdf

140 https://fairplayalliance.org/wp-content/uploads/2020/12/FPA-Framework.pdf

141 Fair Play Alliance and Anti-Defamation League‘s Center for Technology and Society. (2020.) ”Disruption and Harms in Online Gaming Framework”. Fair Play Alliance and Anti-Defamation League‘s Center for Technology and Society. Retrieved from https://fairplayalliance.org/wp-content/uploads/2020/12/FPA-Framework.pdf

142 Fair Play Alliance. (n.d.) ”Webinars”. Fair Play Alliance. Retrieved from https://fairplayalliance.org/webinars/

143 Global Internet Forum to Counter Terrorism (n.d.). ”About”. Global Internet Forum to Counter Terrorism. Retrieved from https://gifct.org/about/

144 Global Internet Forum to Counter Terrorism. (n.d.). ”GIFCT’s Hash-Sharing Database”. Global Internet Forum to Counter Terrorism. Retrieved from https://gifct.org/hsdb/; Global Internet Forum to Counter Terrorism. (n.d.). ”Content Incident Protocol”. Global Internet Forum to Counter Terrorism. Retrieved from https://gifct.org/content-incident-protocol/

145 Shaikh, Shiraz. (2024). ”Gaining Steam: Far-Right Radicalisation on Gaming Platforms”. Global Network on Extremism & Technology. Retrieved from https://gnet-research.org/2024/07/29/gaining-steam-far-right-radicalisation-on-gaming-platforms/

146 Tech Against Terrorism. (n.d.). ”How We Work”. Tech Against Terrorism. Retrieved from https://techagainstterrorism.org/how-we-work

147 Tech Against Terrorism. (n.d.). ”Mentorship”. Tech Against Terrorism. Retrieved from https://techagainstterrorism.org/mentorship-for-tech-platforms

148 Tech Against Terrorism. (2023). ” State of Play: Trends in Terrorist and Violent Extremist Use of the Internet 2022”. Tech Against Terrorism. Retrieved from https://techagainstterrorism.org/news/2023/01/19/state-of-play-trends-in-terrorist-and-violent-extremist-use-of-the-internet-2022

149 Family Online Safety Institute. (n.d.). ”About FOSI”. Family Online Safety Institute. Retrieved from https://www.fosi.org/about-fosi

150 Family Online Safety Institute. (n.d.). ”Safer Gaming Guide”. Family Online Safety Institute. Retrieved from https://www.fosi.org/good-digital-parenting-resource/safer-gaming-guide

151 Rosenblat, Mariana Olaizola. (2023). “How Russia Is Using Online Video Games to Promote the War in Ukraine”. Just Security. Retrieved from https://www.justsecurity.org/87566/how-russia-is-using-online-video-games-to-promote-the-war-in-ukraine/

152 Riot Games. (2022). ”An Update on Player Dynamics”. Riot Games. Retrieved from https://www.riotgames.com/en/news/an-update-on-player-dynamics

153 Rosenblat, Mariana Olaizola and Paul M. Barrett. (2023). ”Gaming The System: How Extremists Exploit Gaming Sites And What Can Be Done To Counter Them”. NYU Stern Center for Business and Human Rights. Retrieved from https://bhr.stern.nyu.edu/wp-content/uploads/2024/01/NYUCBHRGaming_ONLINEUPDATEDMay16.pdf

154 Ibid.

155 Riot Games. (2022). ”An Update on Player Dynamics”. Riot Games. Retrieved from https://www.riotgames.com/en/news/an-update-on-player-dynamics

156 Modulate. (2024). ”Modulate and Activision Case Study”. Modulate. Retrieved from https://www.modulate.ai/case-studies/modulate-activision-case-study

157 Blizzard. (2024). “Defense Matrix Season 9 Update – Endorsing Positive Players”. Blizzard. Retrieved from https://overwatch.blizzard.com/en-us/news/24056254/defense-matrix-season-9-update-endorsing-positive-players/

158 Rosenblat, Mariana Olaizola and Paul M. Barrett. (2023). ”Gaming The System: How Extremists Exploit Gaming Sites and What Can Be Done to Counter Them”. NYU Stern Center for Business and Human Rights. Retrieved from https://bhr.stern.nyu.edu/wp-content/uploads/2024/01/NYUCBHRGaming_ONLINEUPDATEDMay16.pdf

159 Ibid.

160 Fair Play Alliance and ADL. (2020). ”Disruption and Harms in Online Gaming Framework”. Fair Play Alliance. Retrieved from https://fairplayalliance.org/wp-content/uploads/2020/12/FPA-Framework.pdf

161 Saltman, Erin and Nagham El Karhili. (2024). ”Level Up: Policies, Practices, and Positive Interventions to Counter Terrorism and Violent Extremism in Gaming Spaces”. Gaming and Extremism.
Retrieved from https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003388371-10/level-erin-saltman-nagham-el-karhili?context=ubx&refId=0dad8f3a-ddd9-4696-8081-4b29013af34b

162 Twitch. (n.d.). ”Community Guidelines”. Twitch.
Retrieved from https://safety.twitch.tv/s/article/Community-Guidelines?language=en_US

163 Lakhani, Suraj. (2021). ”Video Gaming and (Violent) Extremism: An exploration of the current landscape, trends, and threats”. European Commission. Retrieved from https://home-affairs.ec.europa.eu/document/download/67db2a03-5b45-44f2-b0e9-3b0544a08dfc_en?filename=EUIF%20Technical%20Meeting%20on%20Video%20Gaming%20October%202021%20RAN%20Policy%20Support%20paper_en.pdf

164 Office of Representative Lori Trahan. (2023). ”Summary Of Responses from Gaming Companies”. Office of Representative Lori Trahan.
Retrieved from https://trahan.house.gov/uploadedfiles/summary_responses_to_letter_game_companies_online_harassment_extremism.pdf

165 Rosenblat, Mariana Olaizola and Paul M. Barrett. (2023). ”Gaming The System: How Extremists Exploit Gaming Sites And What Can Be Done To Counter Them”. NYU Stern Center for Business and Human Rights.
Retrieved from https://bhr.stern.nyu.edu/wp-content/uploads/2024/01/NYUCBHRGaming_ONLINEUPDATEDMay16.pdf

166 Ibid.

167 Ibid.

168 Hartgers, Menso and Eviane Leiding. (2023). ”Fighting extremism in gaming platforms: a set of design principles to develop comprehensive P/CVE strategies”. International Centre for Counter-Terrorism. Retrieved from https://www.icct.nl/publication/fighting-extremism-gaming-platforms-set-design-principles-develop-comprehensive-pcve

169 Ibid.

170 Rosenblat, Mariana Olaizola and Paul M. Barrett. (2023). ”Gaming The System: How Extremists Exploit Gaming Sites And What Can Be Done To Counter Them”. NYU Stern Center for Business and Human Rights.
Retrieved from https://bhr.stern.nyu.edu/wp-content/uploads/2024/01/NYUCBHRGaming_ONLINEUPDATEDMay16.pdf

171 Ibid.

172 Schlegel, Linda. (2024). ”Preventing and Countering Extremism in Gaming Spaces”. Gaming and Extremism.
Retrieved from https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003388371-11/preventing-countering-extremism-gaming-spaces-linda-schlegel?context=ubx&refId=ea1a23f6-d915-40f5-8f21-bab73bf085b5

173 Ibid.

174 Ibid.

175 Anti-Defamation League’s Center for Technology and Society (2024).
”Hate is No Game: Hate and Harassment in Online Games 2023”. Anti-Defamation League.
Retrieved from https://www.adl.org/resources/report/hate-no-game-hate-and-harassment-online-games-2023

176 Lamphere-Englund, G. & White, J (May 2023). “The Online Gaming Ecosystem: Assessing Socialisation, Digital Harms, and Extremism Mitigation Efforts”. Global Network on Extremism and Technology (GNET). p. 19.
Retrieved from https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf

177 Australia. (2021). “Online Safety Act 2021, No. 76, 2021, Compilation No. 1”. Australia.
Retrieved from: https://www.legislation.gov.au/C2021A00076/latest/text

ALFRED LANDECKER
FOUNDATION

ISD | Powering solutions to extremism, hate and disinformation

Amman | Berlin | London | Paris | Washington DC

www.isdglobal.org